AD-A271 628



GACIAC SR-93-01



AMC-SWMO COUNTERMEASURES STUDY

Volume I: Guide to How Countermeasures
Affect Smart Weapons





S DTIC ELECTE DOCT 2 6 1993 D

Original contains color plates: All DTIC reproductions will be in black and white

Published by GACIAC IIT Research Institute 10 West 35th Street Chicago, IL 60616-3799

FOURTH PRINTING JUNE 1993 APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED

93 10 22 07 2

NOTICES

Special Report. This special report has been published by the Guidance and Control Information Analysis Center (GACIAC) as a service to the defense community. GACIAC is a DoD Information Analysis Center, administered by the Defense Technical Information Center, operated by IIT Research Institute under Contract No. DLA-900-86-C-0022. GACIAC is funded by DTIC, DARPA and U.S. Army, U.S. Navy, and U.S. Air Force Laboratories/Controlling Activities having an interest in weapon guidance and control. The Director of GACIAC is Dr. Robert J. Heaston. The Contracting Officer is Ms. Cheryl Montoney, DESC, Dayton, Ohio. The Contracting Officer's Technical Representative is Mr. Chalmer D. George, and the Alternate Representative is Mr. H.C. Race, U.S. Army Missile Command, AMC Smart Weapons Management Office, Attn: AMSMI-SW, Redstone Arsenal, Alabama 35898-5222.

Reproduction. Permission to reproduce any material contained in this document must be requested from and approved in writing by the U.S. Missile Command, AMC Smart Weapons Management Office, Attn: AMSMI-SW, Redstone Arsenal, Alabama 35898-5222. This document is only available from GACL. C, IIT Research Institute, 10 West 35th Street, Chicago, Illinois 60616-3799. Copies are available to Government agencies under service supplementary core funding and GACIAC industrial subscribers. Cost to others as indicated in block 16 of the inclosed Standard Form 298 (page i), are authorized to offset reproduction and distribution costs by GACIAC.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and mainteining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information including suggestions for reducing the burden, to Washington Headquerters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE Reprinted June 1		REPORT TYPE AND DATES COVERED Special Report; 19 June 1989
4. TITLE AND SUBTITLE AMC-SWMO Countermeasures St Volume I: Guide to How Countern		Weapons	5. FUNDING NUMBERS DLA900-86-C-0022
6. AUTHOR(S) Eric J. Borg, Paul Lavalee, James and Thomas C. Weaver			PE 65805
7. PERFORMING ORGANIZATION NAME(S) A Dynetics, Inc. W & G Si 1000 Explorer Blvd. 3322 Sout Huntsville, AL 35806 Huntsville	igma Services, Inc. h Memorial Parkway		8. PERFORMING ORGANIZATION REPORT NUMBER GACIAC SR-93-01 Volume I
9. SPONSORING/MONITORING AGENCY NA US Army Missile Command AMC Smart Weapons Managemer Attn: AMSMI-SW			10. SPONSORING/MONITORING AGENCY REPORT NUMBER
Redstone Arsenal, AL 35898-5222 11. SUPPLEMENTARY NOTES This document is available only fr 10 West 35th Street, Chicago, IL	om GACIAC, IIT Res		AD-E-951917 ute,
12a. DISTRIBUTION/AVAILABILITY STATEM Approved for public release; distri			12b. DISTRIBUTION CODE
smart weapon sensors are affected be devices, techniques, or actions that volume will be threat CMs and ho environment. The focus is on the signature alteration, decoys, and dece addition to a technical discussion of the design, analysis, requirements defended responsibilities of various Government currently exists. Guidelines and supprogram manager (PM) in ensuring the	respond to a specific w US Army smart we technical details of the eption, obscurants, and CM classes, the processinition, and testing of ent agencies involved ggestions are presented that more CM robust some involved in the small precision guided me countermeasures, Lase	Ms) on the weapon ac weapons can treat CM cl jammers a less by which smart weapon in the CM and disconart weapon art weapon cunitions, C	· · · · · · · · · · · · · · · · · · ·
17. SECURITY CLASSIFICATION 18. SEC	URITY CLASSIFICATION THIS PAGE	19. SECURIT	Y CLASSIFICATION 20. LIMITATION OF

NSN 7540-01-280-5500

Unclassified/Unlimited

Unclassified

Unclassified

Unclassified

AMC-SWMO COUNTERMEASURES STUDY

Volume I: Guide to How Countermeasures Affect Smart Weapons

Approved for Public Release: Distribution Unlimited

Published by GACIAC IIT Research Institute 10 West 35th Street Chicago, Illinois 60616-3799

> FOURTH PRINTING JUNE 1993

Acception For

NTIS CRA&I V
PHO IAB ID
Unanaborized ID
Untribution |

Availability Codes

Dist Available and or Special

A-I 2

GACIAC - A DoD Information Analysis Center
Operated by IIT Research Institute, 10 West 35th Street, Chicago, Illinois 60616-3799
DoD Technical Sponsor-Joint Service Guidance and Control Committee
Members from OSD, Army, Navy, Air Force and DARPA

FOREWORD

The recent success of smart weapons during Operation Desert Storm has focused attention on the capabilities and performance of this modern family of weapon systems. In the future, our increased reliance on these smart weapons will inevitably be accompanied by the development, on the part of our adversaries, of more sophisticated means of degrading the overall effectiveness of these weapon systems. These countermeasures, which include devices, techniques or actions designed to reduce overall system effectiveness, must be thoroughly understood by all involved in the smart weapons development/acquisition process. This volume, the first in a series initiated by the Army Materiel Command - Smart Weapons Management Office, is designed to address the many complex issues associated with smart weapons countermeasures.

This specific report is intended for both the smart weapons materiel developer and combat developer. It addresses the basic issues associated with the development of smart weapons that are designed to function and survive in a modern countermeasure environment. The overall objectives of this volume are twofold: (1) to present a generic tutorial on the basic issues related to the effects of countermeasures on smart weapons, and (2) to introduce the organizations, primarily within the Army, who are key players in the specification, development, and evaluation of smart weapons countermeasures. Specifically highlighted are the United States Army Survivability Management Office, Vulnerability Assessment Laboratory, and the Vulnerability/Lethality Assessment Management Office who have shared in preparation of this document.

Colonel Robert L. Friedrich

Director

Army Materiel Command - Smart Weapons Management Office

PREFACE

The Army Materiel Command Smart Weapons Management Office (AMC-SWMO) has prepared a series of publications defining CM/CCM robustness assessment methodology, which they would like to make available to a broader audience. Three publications are involved:

- AMC-SWMO Countermeasures Study, Volume I: Guide to How Countermeasures Affect Smart Weapons (Unclassified/Unlimited)
- AMC-SWMO Countermeasures Study Volume II: Effects of Countermeasures on Smart Weapons Technology (Secret)
- AMC-SWMO Countermeasures Study, Volume IV: Guide to Army Smart Weapon Testing Issues (Unclassified/Unlimited)

These three volumes are being reprinted by the Guidance and Control Information Analysis Center (GACIAC) at the request of SWMO. All three are being published as separate volumes of a GACIAC Special Report (SR) which is numbered GACIAC SR-93-01. Each of the volumes was prepared by different authors; their results are being published as released by AMC-SWMO.

There is a Volume III in this countermeasures series but it is classified and is for controlled distribution (by permission only). Volume III discusses countermeasures against five specific weapon systems and contains an Executive Summary of the overall AMC-SWMO Countermeasures Study. The five systems discussed under Volume III are:

- Vol III-A: Sense & Destroy Armor (SADARM) (Secret)
- Vol III-B: Smart Target Activated Fire and Forget (STAFF) (Secret/NF)
- Vol III-C: Non-Line of Sight Anti-Tank (NLOS-AT) (Secret/NF)
- Vol III-D: MLRS-Terminal Guidance Warhead (MLRS-TGW) (Secret)
- Vol III-E: Generic LADAR Anti-Armor System (GLAAS) (Secret)

If anyone would like more details on Volume III, please contact the GACIAC Contracting Officers Technical Representative (COTR) at the following AMC-SWMO address:

Commander
US Army Missile Command
Attn: AMSMI-SW (Chalmer D. George)
Redstone Arsenal, AL 35898-5222

Dr. Robert J. Heaston Director of GACIAC

ABSTRACT

This volume provides background technical and programmatic information on the complex subject of how smart weapon sensors are affected by countermeasures (CMs) on the battlefield. This report defines CMs as devices, techniques, or actions that respond to a specific weapon action or capability. The subject of this volume will be threat CMs and how US Army smart weapons can be made to be more robust in a CM environment. The focus is on the technical details of threat CM classes. These classes are designated as: signature alteration, decoys and deception, obscurants, and jammers and directed-energy weapons (DEWs). In addition to a technical discussion of CM classes, the process by which the Army incorporates CM effects into the design, analysis, requirements definition, and testing of smart weapons will also be discussed. The roles and responsibilities of various Government agencies involved in the CM assessment process are presented as it currently exists. Guidelines and suggestions are presented and discussed to assist the smart weapon system program manager (PM) in ensuring that more CM robust smart weapons are developed. Although the PM is the primary focus of this volume, everyone involved in the smart weapon and CM planning process should benefit from the information provided.

EXECUTIVE SUMMARY

This guide provides background technical and programmatic information on the complex subject area of how smart weapon sensors can and must function in the presence of CMs on the future battlefield. It is one of several documents sponsored by the Army Materiel Command Smart Weapons Management Office (AMC-SWMO) as part of a comprehensive review of smart weapons in realistic, dirty, CM-intense environments. Future volumes will address effects on specific systems and system constructs. Volume III, parts A through E will cover Search and Destroy Armor Munition (SADARM), Smart Target Activated Fire and Forget (STAFF), Non-Line-Of-Sight (NLOS), Multiple-Launch Rocket System-Terminal Guidance Warhead (MLRS-TGW), and a generic laser radar system, respectively.

This unclassified guide is best summarized by the foldout chart in Appendix D: Countermeasure Effects on Smart Weapon Sensors. Although the concentration is on smart weapon sensors, the chart and this guide both provide general information on definitions, organizations, and issues relevant to system survivability (the ability to avoid or withstand the effects of enemy action and continue the mission). The CM executive chart serves as a foundation to this subject.

This guide builds on that foundation to provide additional, specific insights for the smart weapon combat and materiel developers, and their Government and contractor support teams throughout the

research, development, test, and evaluation (RDT&E) community. The discussions on electromagnetic (EM) effects, smart weapon design and employment considerations, and program planning and documentation issues will serve as a refresher, checklist, or tutorial depending on the reader's experience with both smart weapons and CMs. Additional details on technical aspects of CM/smart weapon interactions are contained in the classified companion volume: "Effects of CMs on Smart Weapons Technology."

The AMC-SWMO has dedicated these efforts to ensure that realistic CMs are included in all the smart weapon RDT&E phases and processes. This guide is the initial step to more clearly define CM issues for the smart weapon RDT&E community (from component designers to senior decision makers) and to provide expanded support to that community in the development of their products. CM processes and programs are multifaceted. Adequate inclusion of cost-effective CM solutions in the technology-driven, autonomous, miniaturized smart weapon designs requires a coordinated team effort, especially in smart weapon RDT&E programs.

THE CM SOLUTION IS A COMMUNITY EFFORT

TABLE OF CONTENTS

				Page
1.	INT	RODUC	TION	1-1
	1.1	PURP	OSE	. 1-1
	1.2	SCOP	E	. 1-2
	1.3	ORGA	NIZATIONS	1-2
	1.4	TECH	NICAL APPROACH	.1-4
	1.5	GUIDE	TO VOLUME I	1-5
2.	SMA	ART WE	APONS OVERVIEW	2-1
	2.1	SMAR	T WEAPONS DEFINITION AND CATEGORIES	2-1
		2.1.1	Types of Smart Weapons	2-1
		2.1.2	Battlefield Employment of Smart Weapons	2-1
	2.2	SMAR	T WEAPCN SYSTEMS SUMMARY	2-2
	2.3	SMAR	T WEAPON FUNCTIONS	2-6
	2.4	SMAR	T WEAPONS SURVIVABILITY VERSUS VULNERABILITY	2-7
		2.4.1	Evaluating System Vulnerability	2-8
		2.4.2	Survivability Considerations	2-10
		2.4.3	Assessing Cost-Effectiveness	2-10
3.	COL	INTERN	MEASURES OVERVIEW	3-1
	3.1	COUN	TERMEASURES - A DOUBLE-EDGED SWORD	3-1
		3.1.1	Classes of CMs	3-2
		3.1.2	Categories of CMs	3-4
	3.2	CM EF	FECTS AND EMPLOYMENT	3-5
		3.2.1	CM Effects and CCM Reaction	3-5
		3.2.2	Range of CM Effects	3-6

TABLE OF CONTENTS (Continued)

				Page
		3.2.3	Tactics, Techniques, and Procedures	3-8
	3.3	BATT	LEFIELD EMPLOYMENT OPPORTUNITIES	3-10
4.	COL	JNTER	MEASURE EFFECTS ON SMART WEAPONS	4-1
	4.1	SIGN	ATURE ALTERATION	4-1
		4.1.1	Visual Signature Alteration	4-4
		4.1.2	IR Signature Alteration	4-5
		4.1.3	MMW Signature Alteration	4-8
	4.2	DECC	DY/DECEPTION	4-9
		4.2.1	Visual and IR Decoys	4-10
		4.2.2	MMW Decoys	4-11
	4.3	OBSC	URANTS	4-12
		4.3.1	Visual and IR Obscurants	4-13
		4.3.2	MMW Obscurants	4-14
	4.4	JAMM	ERS AND DEWs	4-18
		4.4.1	Jammers	4-19
		4.4.2	DEWs and Projectiles	4-21
5.	ENH	IANCIN	IG SMART WEAPON EFFECTIVENESS IN A CM ENVIRONMENT	5-1
	5.1	SMAR	T WEAPON CCM TECHNIQUES	5-1
		5.1.1	Countering CM Effects	5-1
		5.1.2	Countering CM Functions	5-2
	5.2	SMAR	T WEAPON HARDWARE/SOFTWARE DESIGN	5-4
	53	SMAR	T WEAPON EMPLOYMENT AND ENGAGEMENT OPTIONS	5-6

TABLE OF CONTENTS (Concluded)

			rage
6.	SMA	RT WEAPON CM PROGRAM PLANNING ISSUES	. 6-1
	6.1	REQUIREMENTS AND SYSTEM SPECIFICATION DEFINITION	6-1
	6.2	SYSTEM DESIGN SUPPORT	6-4
	6.3	TESTING ISSUES	6-5
	6.4	CM AND WEATHER AVAILABILITY ANALYSIS	6-6
7.	SUMI	MARY	7-1
RE	FERE	NCES	R-1
AF	PEND	IX A. INDEX TO KEY POINTS	. A-1
AP	PEND	DIX B. ACRONYMS AND DEFINITIONS	B-1
AF	PEND	IX C. RESOURCE ORGANIZATIONS	.C-1
	C.1	INTRODUCTION	C-3
	C.2	ARMY MATERIEL COMMAND - SMART WEAPONS MANAGEMENT OFFICE (AMC-SWMO)	C-3
	C.3	ARMY MATERIEL SYSTEMS ANALYSIS ACTIVITY (AMSAA)	C-4
	C.4	ATMOSPHERIC SCIENCES LABORATORY (ASL)	C-4
	C.5	CHEMICAL RESEARCH, DEVELOPMENT, ENGINEERING CENTER (CRDEC)	C-5
	C.6	CHICKEN LITTLE JOINT PROGRAM OFFICE (CL JPO)	C-6
	C.7	HARRY DIAMOND LABORATORIES (HDL)	C-6
	C.8	SURVIVABILITY MANAGEMENT OFFICE (SMO)	C-8
	C.9	VULNERABILITY ASSESSMENT LABORATORY (VAL)	C-8
	C.10	VUNERABILITY/LETHALITY ASSESSMENT MANAGEMENT OFFICE (VLAMO)	C-9
	C.11	3246 TEST WING, EGLIN AIR FORCE BASE	C-9
ΔΡ	DENID	IX D. EXECUTIVE CHART	D-1

LIST OF ILLUSTRATIONS

<u>Figure</u>	<u>Title</u>	<u>Page</u>
1-1	The Army Countermeasure and Survivability Community	1-3
1-2	Outline of Report	1-6
2-1	Guided Munition Weapon System Operational Scenario	2-2
2-2	Smart Munition Weapon System Operational Scenario	2-3
2-3	Smart Weapon Systems of Interest	. 2-4
2-4	Smart Weapon Systems Data Links	. 2-5
2-5	Elements of System Vulnerability	. 2-9
3-1	Normal Progression of CM and CCM Actions	3-2
3-2	Hull Defilade Types	. 3-9
4-1	Relative Impact of CM Types	. 4-2
4-2	Smart Weapon CM Techniques	. 4-4
4-3	IR Emissivity and Reflectivity	. 4-5
4-4	ΔT Definitions	. 4-7
4-5	MMW Reflection at Different Boundaries	. 4-8
4-6	IR Decoy Temperature and Spectral Ratios	. 4-10
4-7	Effects of Obscurants on Smart Weapons	. 4-12
4-8	Concentration Length of an Obscurant	. 4-14
4-9	How Chaff is Used on the Battlefield	. 4-18
4-10	Jammers and DEWs on the Battlefield	. 4-18
5-1	Examples of Countering the CM Function	. 5-3
5-2	TGSM Many-on-Many Engagement Scenario	. 5-8
6-1	Typical CM Process	. 6-2
6-2	Acquisition Documents With CM Annexes	6-3
6-3	The Difficulty in Stating Clear Availability Requirements	6-7

LIST OF TABLES

<u>Table</u>	<u>Title</u>	<u>Page</u>
3-1	Classes of EW CMs to Smart Weapon Sensors	3-3
3-2	Categories of Threat CMs	3-5
3-3	Samples of CM/CCM Reactions to Smart Weapons Designs	3-6
3-4	Typical Effects from DEWs	3-7
4-1	Mass Extinction Coefficients for Combat-Induced Obscurants	4-16
4-2	Radar Attenuation for Carbon Fiber Chaff	4-18
5-1	Examples of Potential Ways of Countering CM Effects	5-2
6-1	Strawman CM and Weather Availability Matrix	6-9
C-1	EOSAEL Modules	C-4
C-2	Example Listing from AAODL Expanded Index	C-6

LIST OF ABBREVIATIONS

α Mass extinction coefficient describes the radiation scattering ability of smoke particles.

AAODL Atmospheric Aerosol and Optics Data Library

AAWS-M Advanced Antitank Weapon System - Medium (became Javelin)

AGC automatic gain control
AIA Army Intelligence Agency

AMC-SWMO Army Materiel Command Smart Weapons Management Office

AMCCOM Armaments, Munitions, and Chemical Command
AMSAA Army Materiel Command Systems Analysis Activity

APGM Autonomous Precision Guided Munition
ASARC Army System Acquisition Review Council

ASL Atmospheric Sciences Laboratory
ASM Armored Systems Modernization
BDA Battle Damage Assessment
BDP Battlefield Development Plan

BICT Battlefield Induced Contaminants Test

BRL Ballistics Research Laboratory

C³I command, control, communications, and intelligence CAC Combined Arms Command (previously Center)

CCM counter-countermeasure CG Commanding General

CL concentration length or Chicken Little
CL JPO Chicken Little Joint Project Office

CM countermeasure

CNVEO Center for Night Vision and Electro-Optics COEA cost and operational effectiveness analysis

CO₂ carbon dioxide

COMBIC Combined Battlefield Induced Obscurations Code

CRDEC Chemical Research, Development, and Engineering Center

CW continuous wave

DA Department of the Army
DAB Defense Acquisition Board
DCG Deputy Commanding General

DCGRDA Deputy Commanding General for Research, Development, and Acquisition

DCSINT Deputy Chief of Staff for Intelligence

DEW directed energy weapon DF deuterium fluoride

DMEWS Directed Microwave Energy Weapon Simulation

DoD Department of Defense

DPICM dual-purpose improved conventional munitions

ECCM electronic counter-countermeasure

ECM electronic countermeasure EFP explosively formed penetrator

EM electromagnetic

EMD engineering and manufacturing development

EME electromagnetic effects
EMI electromagnetic interference

EO electro-optic

EOSAEL Electro-Optic Systems Atmospheric Effects Library
ETDL Electronics Technology and Devices Laboratory

LIST OF ABBREVIATIONS (Continued)

EW electronic warfare

EWVA Electronic Warfare Vulnerability Assessment

FAR false alarm rate

FID Foreign Intelligence Division
FIO Foreign Intelligence Office

FITTE fire-induced transmission and turbulence effects

FLIR forward-looking infrared

FOV field of view

GACIAC Guidance and Control Information and Analysis Center

G&C guidance and control GM guided munition

HC Hexachloroethane (type of smoke)
HDL Harry Diamond Laboratories

HE high explosive
HEL high-energy laser
HF hydrogen fluoride
HOJ home-on-jam

HPM high power microwave
IFOV instantaneous field of view
IOC initial operational capability
IR infrared: 1 to 14 microns

IRTGSM Infrared Terminally Guided Submunition
JMSNS Justification for Major System New Start

JSGCC Joint Services Guidance and Control Committee

JTCG-ME Joint Technical Coordinating Group for Munitions Effectiveness

L radiance (W/cm²-sr)
LABCOM Laboratory Command

LEL low-energy laser LOS line-of-sight

LOSAT line of sight antitank
LWIR long wave infrared
MAA Mission Area Analysis
MICOM Missile Command

MLRS-TGW Multiple Launch Rocket System - Terminal Guidance Warhead

MMW millimeter wave

MTL Materials Technology Laboratory

MWIR mid-wave infrared

NADR National Armor/Anti-Armor Data Repository Nd:YAG neodymium: yttrium aluminum garnet

NG/FS next generation/future system

NLOS non-line-of-sight

OPTEC Operational Test and Evaluation Command

ORD Operational Requirements Document

OSD Office of Secretary of Defense pre-planned product improvement

PAT Process Action Team
PEO Program Executive Office
PGM precision guided munition

LIST OF ABBREVIATIONS (Concluded)

PIP Product Improvement Program

PM Program Manager POC point of contact

R&D research and development radar absorbing material radar cross section

RDEC Research, Development, and Engineering Center research, development, test, and evaluation

RF radio frequency RGPO range gate pull-off

ROC required operational capability
SADARM Search and Destroy Armor Munition
SEMI Special ElectroMagnetic Interference

SFM sensor fuzed munition

SM smart munition

SMO Survivability Management Office

SOJ standoff jammer

STAFF Smart Target Activated Fire and Forget STAR System Threat Assessment Report

SWIR short wave infrared

TABILS Target and Backgro. Information Library System

TACOM Tank Automotive Command
TEMP Test Evaluation Master Plan
TGSM terminally guided submunition
TIWG Test Integration Working Group

TLE target location error

TOW Tube launched Optically tracked Wire Guided

TRAC TRADOC Analysis Command
TRADOC Training and Doctrine Command
TRISIG Tri-Service Signatures Data Base
TSM TRADOC System Manager
UAV unmanned aerial vehicle

VAL Vulnerability Assessment Laboratory

VGPO velocity gate pull-off

VLAMO Vulnerability/Lethality Assessment Management Office

WP white phosphorous

WSMR White Sands Missile Range

Units of Measure

°C degrees Celsius

dB decibels gram GHz gigahertz K Kelvin kg kilograms meters m MHz megahertz millimeters mm micrometers μm

1. INTRODUCTION

1.1 PURPOSE

The objectives of this volume are: (1) to highlight the technical issues related to the generic effects of CMs on smart weapon systems, and (2) to provide an introduction to organizations within the Department of the Army (DA) that are involved in the various aspects of CMs and smart weapons. A CM is a device, technique, or action that responds to a specific enemy action or capability; a CM is designed to reduce an enemy's capability or operational effectiveness. The purpose of a CM against smart weapons is to destroy or degrade the effectiveness of a smart weapon. Counter-countermeasures (CCMs) are devices, techniques, or actions designed to permit a system to function effectively even in the presence of threat CMs. This volume is designed as an unclassified tutorial for wide dissemination among Government and industry personnel involved in the specification, development, test, and evaluation of smart weapons and their CMs. The document provides an understanding and appreciation of how smart weapons can be developed to function properly and survive a CM environment on future battlefields. It is designed to serve engineers and managers in the project offices and program executive offices. The document is also useful to others in the community, such as combat developers and key decision makers. The information contained in this document is also useful in planning test programs and special evaluations.

This guide highlights the roles of the Survivability Management Office (SMO), Vulnerability/ Lethality Assessment Management Office (VLAMO), Vulnerability Assessment Laboratory (VAL), and other agencies and offices involved in CMs for smart weapons. This document does not provide a blanket requirement for CMs on smart weapons nor a blanket assessment of the vulnerability of smart weapons to CMs. It provides the development community with information that will ensure that specifications and requirements are meaningful to their system and that the design implications of vulnerability assessments are fully understood.

This guide should be used by senior PM/Program Executive Officer (PEO) personnel who are interest. In gaining a better appreciation of the CMs and the effects they can have on smart weapons. Staff officers and engineers in the engineering management and test management divisions should use this document as a basic reference for terms, issues, and concepts as well as a guide to available models and resource agencies. Personnel in combat development and DA staff positions can benefit in a similar manner. Finally, supporting Research, Development, and Engineering Centers (RDECs) and prime contractors should find this document useful for engineers and specialists who are developing smart weapons and CMs.

1.2 SCOPE

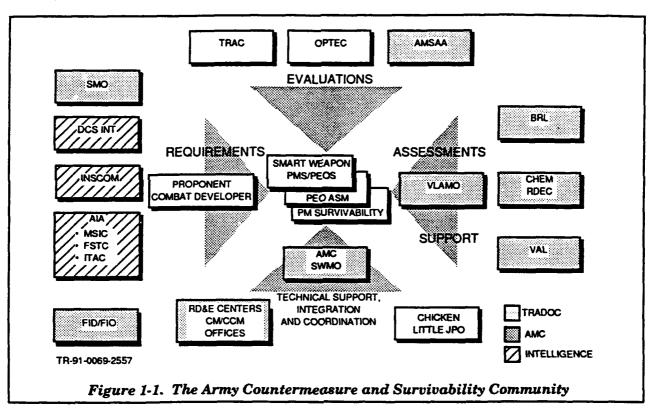
This volume addresses the fundamental effects of CMs on smart weapon seekers and sensors. It focuses on the impact of CMs on the functions of launch, dispense, acquisition, hit, and kill. The discussion is outlined in the acquisition and hit functions, but CM effects on dispense and kill are also covered as they relate to sensors and seekers. Therefore, this document focuses more on functional survivability, and less on physical survivability. Finally, since this document is intended for the smart weapon material developer, the emphasis is on material CMs. Tactics and doctrine used by the threat as a CM are only covered incidentally as this subject is better addressed by the combat developer.

1.3 ORGANIZATIONS

The issue of specifying, assessing, evaluating, and testing CM effects on smart weapons is a responsibility shared by numerous agencies across many major commands. No single organization is solely responsible for ensuring the survivability of smart weapons in a CM environment. *Figure 1-1* shows the CM and survivability community within the Army at the top-most organizational levels. The issues of smart weapon survivability are complex, involving assessment of threat projections, technical design issues, physical phenomena, force effectiveness impact, and cost benefit analysis. However, the smart weapon PM is clearly the central player in these issues. The smart weapon PM will have the greatest influence on how the smart weapon is built to survive on the battlefield. The importance of the PM and his staff cannot be overlooked as they are actively involved in all aspects of this process, and for this reason, they receive the majority of the attention of this volume.

Figure 1-1 depicts the CM/survivability community as four general groups of organizations providing CM requirements (specification), assessments (testing and analysis), evaluations, and technical support. It should be noted that the placement of organizations into these categories was to provide a basic idea of their primary role in this process. These organizations are not limited to these roles. Many organizations have review and coordination roles on multiple CM aspects. Central to this process are the PMs and PEOs developing smart weapon systems. In addition, the PEO for Armored Systems Modernization (ASM) and the PM for Survivability Systems are included to acknowledge the two-edge sword of CMs. An effective CM against a blue smart weapon can also be an effective protection for blue vehicles against threat smart weapons. The analysis of foreign weapons systems by the intelligence community includes projections of CM systems and techniques on the battlefield. These general projections are reviewed and classified as threats based on the specific US smart weapons system under consideration. This system-specific threat listing process results in the production and updating, as required, of the System Threat Analysis Report (STAR). STAR production and STAR maintenance are performed by the Foreign Intelligence Division (FID) of the appropriate commodity command (normally US

Army Missile Command (MICOM) or Armaments, Munitions, and Chemical Command (AMCCOM) for smart weapons). Next, the threat CM list contained in the STAR is incorporated into a requirements document for the weapon system being developed. These data will normally be contained in a Survivability Annex (formerly called the Countermeasures Annex) to the basic Operational Requirements Document (ORD), tormerly called the ROC. The SMO, under the Laboratory Command (LABCOM), has responsibility for preparing the Survivability Annex. This annex is produced in coordination with the Training and Doctrine Command (TRADOC) proponent combat developer (for smart weapons this typically will be field artillery, infantry, armor, air defense, engineers or Combined Arms Command (CAC), Combat Developments). If an ORD does not have a Survivability Annex, it is recommended that the PM request one be prepared by SMO. Thus, the PM documents CM planning requirements and has a rationale for any hardening or other CCMs in his system.



The testing and assessment of CMs on the smart weapon pose a technically intensive problem. For this reason, several laboratories are involved. The US Army VAL has the responsibility for EW susceptibility testing; the Chemical RDEC (CRDEC) provides expertise in the area of battlefield smoke, chaff, and obscurants; and the US Army Ballistic Research Laboratory (BRL) has responsibility for warhead lethality assessments. Although this study focuses on seekers and sensors and not warheads, BRL and lethality issues are mentioned to emphasize the very close relationship between sensors and warhead performance of smart weapons. VLAMO performs the coordination and combined reporting of the

assessments. As the system matures into engineering and manufacturing development (EMD) and operational testing begins, the Operational Test and Evaluation Command (OPTEC) plays a role in the system assessment from the perspective of the user. Other organizations such as the Electronics Technology and Devices Laboratory (ETDL) and Materials Technology Laboratory (MTL) offer technical expertise in their areas of specialty. Harry Diamond Laboratories (HDL) has expertise in fuzing and high power microwave technologies. Human Engineering Laboratory (HEL) has the expertise in human operator related issues. Atmospheric Sciences Laboratory (ASL) provides models, databases, and technical expertise in the area of environmental effects on CM effectiveness. MICOM RDEC, through its Weapon Sciences Directorate has expertise in high energy lasers. Finally, SMO plays a central role in the preparation of the Survivability Annex. Additional details on some of the more pertinent government organizations and their models and databases are provided in Appendix C of this report.

1.4 TECHNICAL APPROACH

In preparing this volume, it became apparent that the subject should be divided into two areas-technical issues and programmatic processes. The technical issues address the physics and engineering principles of the CM effect phenomena and the organizations that are staffed to research such issues. The programmatic processes address the roles and responsibilities of agencies and offices that set requirements, perform assessments, and conduct evaluations. Naturally, some of the same organizations that provide technical expertise will also have programmatic process responsibilities. The emphasis of this study is on the technical issues.

These technical issues include a discussion of the basic physics and engineering principles of applicable CMs and the effects they have on smart weapons. This information is related to how each CM affects traceability to ensure a responsive system design. The SMO coordinates the decision with TRADOC of whether or not a specific CM should be identified in a Survivability Annex. The PM must then make sure that, if identified, the details describing the characteristics of the CM are sufficient. This ensures that the system design properly considers the specific CM and that the system can be tested unambiguously in a CM environment. Further, impact of CMs on the different smart weapon functions and the design alternatives available to the developer are addressed in Sections 4 and 5.

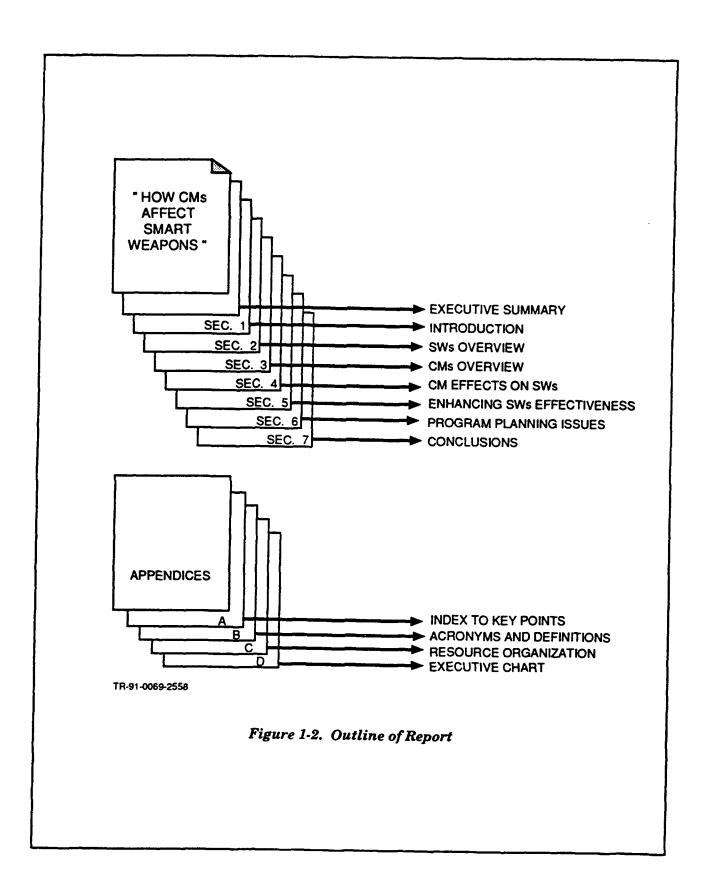
The programmatic processes are discussed for the purpose of showing the applicability of the guide. This discussion includes the basic roles and charters of the various organizations and the acquisition decision process as it relates to CMs and smart weapons. Caution is given that anticipated AMC reorganizations and the initiation of a VAL lead assessment Process Action Team (PAT) may date some of the programmatic processes discussed in this report. However, since many of the procedures are fundamentally required they will probably be retained, perhaps only realigned. The VAL assessment PAT is proposing and staffing for coordination a Department of Defense (DoD) (Tri-Service) EW Vulnerability

Assessment (EWVA) methodology. The EWVA methodology was being formulated as this document was being prepared and therefore, it is not appropriate to include in this study.

1.5 GUIDE TO VOLUME I

An outline of the report is presented in *Figure 1-2*. Section 1 is an introductory section. Sections 2 and 3 contain an overview of smart weapons and CMs, respectively. The purpose of these sections is to present terms, definitions, and concepts that are used later in the volume. Section 4 contains the principal technical discussion of the effects of CMs on smart weapons. The section is broken down by functional CM classes - signature alteration, decoy/deception, obscurants, and special electromagnetic interference (SEMI)/DEWs/jammers. Each section contains a technical description of the CM, a discussion of its impact on smart weapon functions, and an identification of the technical data needed to characterize the CM. Section 5 presents notions and concepts available to the smart weapon developer to resist CMs and maintain effectiveness. Section 6 shows how this guide can be applied to the programmatic processes. The issues discussed include those processes that the PM should perform internally and externally to ensure the development of survivable smart weapons. Section 7 presents a number of study conclusions.

Following the main report are four appendices. Appendix A contains an Index to Key Points of the smart weapon CM process. Appendix B is a glossary of terms and acronyms. Appendix C is a discussion of resource agencies. Appendix D contains a copy of the executive chart, "Countermeasure Effects on Smart Weapon Sensors." The appendix of resource agencies provides a discussion of the support provided on CM/smart weapon issues by several Government organizations. Some of these offices (VLAMO, SMO, etc.) are management offices that have critical programmatic responsibility but are not resourced to provide technical support, models, or data bases. Other organizations have very little, if anything, to do with programmatic processes, but are responsible for the maintenance of DoD approved models and data bases. This appendix summarizes some of the organizations and, if applicable, the model or data base they maintain. Use of these data sources is endorsed by AMC-SWMO, but they should be obtained by contacting the maintaining organization and not AMC-SWMO. Questions regarding points of contact at these organizations can be addressed by AMC-SWMO.



2. SMART WEAPONS OVERVIEW

2.1 SMART WEAPONS DEFINITION AND CATEGORIES

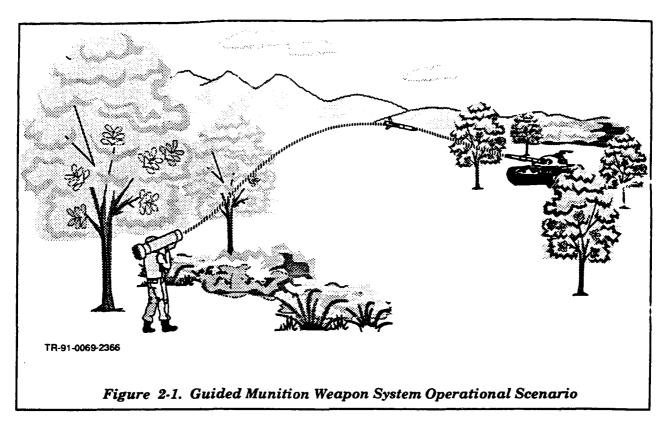
2.1.1 <u>Types of Smart Weapons</u>

Smart weapons are divided into three categories: guided munitions (GM), smart munitions (SM), and brilliant munitions. GMs are characterized as one-on-one munitions that require an opurator in the loop to function. Each munition is directed to a specific target by an operator/soldier. This usually requires a direct line-of-sight (LOS) between the operator (or the sensor being used by the operator) and the target. This need for LOS gives guided munitions the inherent ability to precisely engage specific targets. SMs have the self-contained capability to search, detect, acquire, and engage targets but have minimal capability to discriminate among target classes or target types. They are designed for the many-on-many situation where many munitions are directed into an area known to contain many targets. Brilliant munitions remain in the notional state. It is conceived that these munitions would also operate autonomously, as smart munitions do, however, they would have the capability to selectively identify and engage specific classes of targets.

2.1.2 Battlefield Employment of Smart Weapons

Because a GM normally requires direct LOS and they are able to precisely engage specific targets, they tend to be employed in the close battle. NLOS is unique in that the LOS is maintained between the seeker on the missile and the target rather than the gunner and the target. In this context, NLOS is a guided, indirect-fire munition. An operational scenario, shown in *Figure 2-1*, would consist of a gunner armed with a guided munition, such as the Advanced Antitank Weapon System-Medium (AAWS-M) now designated as Javelin, searching the area for a target. The gunner uses a sight, such as a telescope or infrared (IR) imaging device, for target detection and recognition. Once a target is detected, the gunner aims the sight at the target, so that the missile locks on the target, then fires the weapon. All missile tracking and guidance and control (G&C) functions are performed autonomously. The TOW missile is also a GM; however, once it is fired, the gunner must maintain target lock throughout missile flight.

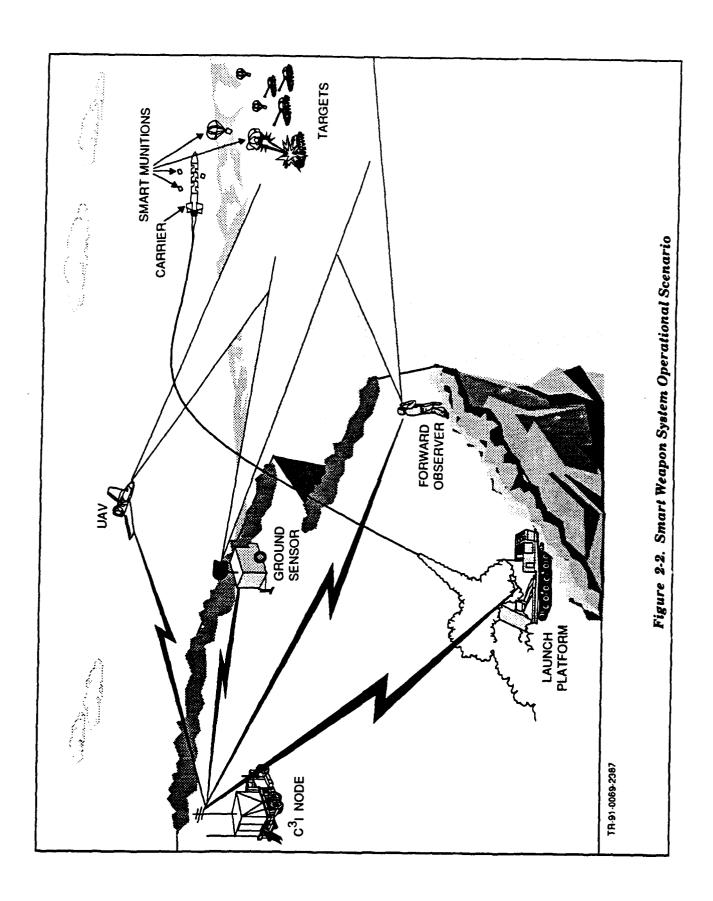
In a SM operational scenario as shown in *Figure 2-2*, a soldier obtains information regarding target type, location, and the specific time of engagement. Target location can originate from any one or a combination of sources. These include aerial and ground sensors, forward observers, or target acquisition/ fire-control equipment onboard the launch platform. The information is forwarded to the firing battery/ launcher via a command, control, communications, and intelligence (C³I) node. The launch platform maneuvers to a specific site before launching the carrier. After launch and flight to the target vicinity, the carrier dispenses the SMs which search for and engage targets.

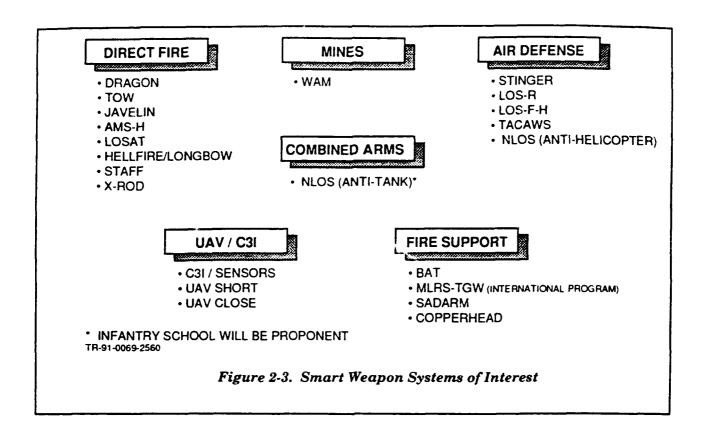


2.2 SMART WEAPON SYSTEMS SUMMARY

The US Army is fielding a variety of smart weapon systems (SADARM, Bat, Javelin, and others). These systems/munitions of interest are shown in *Figure 2-3*. Wire-guided systems, such as TOW and Dragon, require a wire link between the launcher and the missile to transmit guidance commands to the missile. In laser designator systems, a soldier aims a laser designator at the target and the munition tracks on the laser radiation reflected from the target. Examples of laser designator systems are Hellfire and Copperhead.

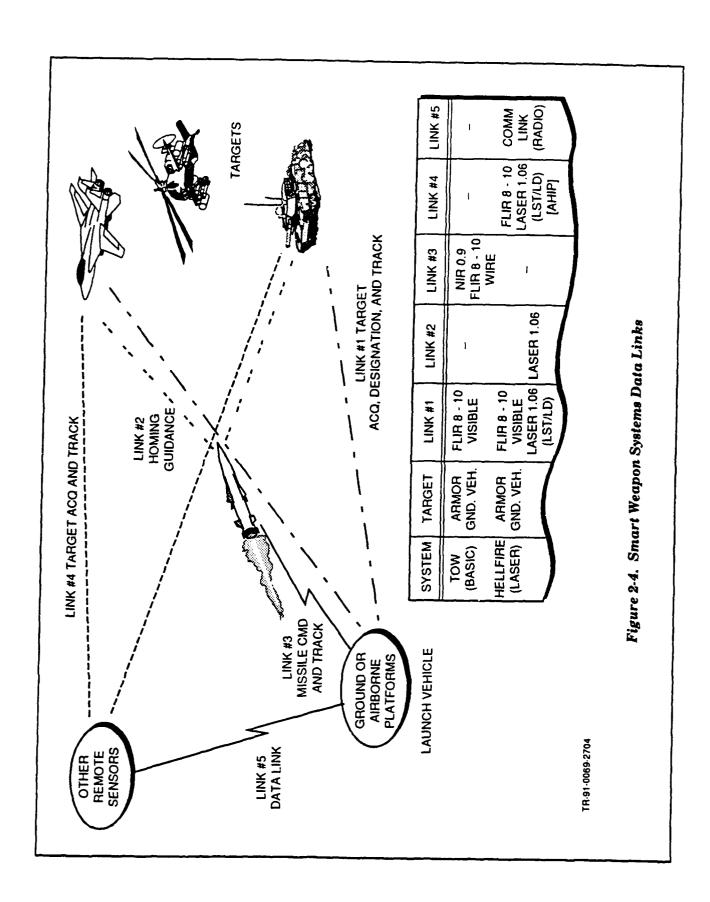
Inherent to each weapon are various data links. *Figure 2-4* depicts the various sensor and data links involved with smart weapon systems. It should be noted that each smart weapon has some, rarely all, of the sensor and data links. The two examples displayed in the figure are typical sets of required data links. To further complicate this generic concept of vital data links, some systems have different sets depending on their employment technique. For example, when the Hellfire missile is fired from a self-designating helicopter, links 4 and 5 in the figure are not present. (Note: Link 3 is never present with Hellfire.) For a remotely designated, lock-on after launch weapon, however, links 4 and 5 are critical, and link 1 is not present.





Also note in *Figure 2-4*, the depicted links may include multiple functions and multiple forms. Hellfire again provides an example for link 1. This link includes the gunner's acquisition and tracking functions using visible or long-wave infrared (LWIR) sights. It also includes the laser designator in the shortwave infrared (SWIR). For more details on smart weapons links, see Volume II of this series, "Effects of Countermeasures on Smart Weapons Technologies," January 1992.

Some smart weapons include an additional, autonomous sensor link between the smart munition in flight and elements of the environment. This sensor link may be as simple as a pressure sensor or attimeter, or as sophisticated as the Navy's Tomahawk's ground scene correlation and tracking. The susceptibility of every data link in the smart weapon system function must be considered in the early design. As will be discussed in the following sections, reductions in basic susceptibility can significantly reduce vulnerability, thus increasing the survivability and effectiveness of the smart weapon. The weapon system can be defeated by eliminating or interfering with any of the links. For example, the Dragon missile track link can be broken under certain levels of smoke. The gunner may see the target through the LWIR sight and subsequently fire the missile. However, while the target is viewed by the gunner, the missile track link, which operates in the SWIR region, cannot transmit through the smoke. Therefore, the missile does not track to the target. The Hellfire laser designator system presents another situation where a specific link can



be defeated. In a smoke environment, either the signal from the laser designator is dissipated by the smoke or the radiation from the laser designator reflects not only from the target but also from the smoke. In the first instance, a missile would not be fired since there is no way to guide the missile to impact. In the other case, a good signal exists to guide the missile; however, if the missile tracks the wrong spot, it flies into the smoke instead of to the target.

2.3 SMART WEAPON FUNCTIONS

While many functions are involved in the successful employment of smart weapons, for the purpose of this study, only the delivery function is examined. The process of delivery consists of launching, dispensing, acquiring, tracking/hitting, and fuzing/killing. The launching function is not addressed in this study because that function is not affected by the CMs that are employed against smart weapon seekers and sensors. The remaining smart weapon functions will be discussed as they are applied to GMs, sensor fuzed munitions (SFMs), and terminally guided submunitions (TGSMs).

In the case of GMs, only the acquiring, tracking/hitting, and fuzing/killing functions are relevant. In the employment of GMs, a human performs the target acquisition and aimpoint designation. In the case of Javelin (AAWS-M), after searching an area and acquiring a target, the gunner selects the aimpoint by sizing gates around the target, locks on the target, then fires the weapon. After firing the weapon, the human is no longer in the loop. The automated functions of aimpoint tracking and missile guidance and control fly the missile to impact. Warhead fuzing is automatic and target kill is position dependent. Position-dependent target kill refers to the position of the hit point on the target, relative to the "shot line" ballistic vulnerability map of the target. Due to the varying degrees of armor thickness and location of critical target components, target kill (for a given warhead) will be a function of the hit location on the target and the angle of attack on the warhead energy. Since a human operator determines or assists in determining the aimpoint, it is harder, but not impossible, to alter the the aimpoint selection and decrease the probability of kill.

For SFMs, only the fuzing/killing process is relevant. The potential for a CM susceptibility during the dispense function is minimal and not further considered. In a simple SFM, when proper thresholds are crossed in the signal processor, the munition is fired. In a complex SFM, fuzing may require multiple looks and combinations of thresholds to verify the presence of a valid target. Further, the aim of the explosively formed penetrator (EFP) may be slightly off the sensor boresight in order to hit a more lethal area on the target. Simple or complex, SFMs only use one function after dispense, the fuzing/kill function. In the context of this report, the fuzing function for SFMs is equivalent to the target acquisition function of TGSMs.

Relevant TGSM functions are dispense, acquisition, track/hit, and fuze/kill. After launch, the carrier delivers the TGSMs to the geographic point at which they will be dispensed. The carrier and TGSMs work together to dispense the TGSMs in an effective dispersal pattern over the target array. For the purpose of this report, the dispense function is responsible not only for stabilizing the TGSM after ejection from the carrier, but also for placing the TGSMs in the proper altitude and attitude to achieve effective

search footprints over the target area. A TGSM that uses a radar altimeter to determine the time to pull up and glide could be susceptible in the dispense function. A jammer could be used by the threat to negate the function of the radar altimeter. If the radar altimeter is jammed, the TGSM no longer knows its altitude above ground; consequently, pullup is affected. Without the proper pullup command, the submunition could fly into the ground or too high for the seeker to acquire targets. Also, since the TGSMs are initially dispensed in a tight cluster, a single beam of energy could irradiate most of the submunitions.

Once dispensed, the TGSMs must search for and acquire targets. Examples of effective CMs against the acquire function are signature alteration, decoys, obscurants, and jamming. After the TGSM acquires a target, it must select an aimpoint, maneuver to that aimpoint, and hit the target to achieve a kill. Tracking to the target is achieved autonomously. Tracking function CMs include signature alteration methods. For an IR TGSM, example methods are hot-spot masking and redirecting of the engine exhaust. For a MMW TGSM, such methods may include the use of materials to lower the target cross section or the use of corner cubes to change the distribution of scatterers on the target.

Subsections 2.2 and 2.3 of this report have described smart weapons in terms of their links and functions. It is important to understand which links and functions are used by the smart weapon being assessed and how they are affected by CMs. A smart weapon is susceptible to a CM, if that CM can negate or degrade one of the links or functions.

2.4 SMART WEAPONS SURVIVABILITY VERSUS VULNERABILITY

In the development of any new system, it is important to determine how the system will operate against a specified array of threat systems. This determination for a smart weapon includes its functional effectiveness against intended targets and its physical survivability - both of which must consider the effects of CMs used by the threat forces. Survivability is the ability to avoid or withstand the effects of enemy action and continue the effective performance of the mission. A weapon system that is easily destroyed or functionally degraded by the enemy has very little utility on the battlefield. Overcoming the threat CMs to the extent that the smart weapon can still function is called "functional survivability". Issues associated with overcoming the destruction, or the threats ability to hit and kill the smart weapon are called "physical survivability" issues. While physical survivability of a weapon is an important issue, in the case of smart weapons, current emphasis is on "functional survivability." This study focuses more on functional survivability issues. For example, an IR seeker on a smart weapon system that cannot discriminate between a real target and a simple decoy will not be very useful. Threat forces can quickly determine a system's weakness and implement appropriate CMs. The implications of countermeasures, such as decoys, and their impact on the ability of a SM to function are key to understanding the role of the SM on tomorrow's battlefield.

"Survivability" and "vulnerability" are, at least for smart weapons, almost the inverse of each other. They are essentially the opposing perspectives of the system's robustness (sum total of survivability)

considering what the threat does to reduce the system's effectiveness (CMs designed to exploit vulnerabilities). To enhance any systems survivability, it is essential that its vulnerability be determined and reduced to an acceptable level. Although "vulnerability" includes ballistic, nuclear, EW, and chemical vulnerabilities, this discussion is limited to negative effects on the smart weapon sensor and/or its function through EW vulnerability.

2.4.1 Evaluating System Vulnerability

Understanding the vulnerability of any system requires an assessment of that system's ability to withstand enemy actions or attacks designed to degrade or defeat it. A typical vulnerability analysis considers the anticipated deployment and use of a given system on the battlefield and addresses the full range of threat systems that can interact with it. Some threat weapon systems can be dismissed early in the vulnerability assessment because of their very limited or unlikely interaction with the system under investigation. Other threat systems or their interaction phenomenology may require laboratory or range testing to adequately assess their effectiveness.

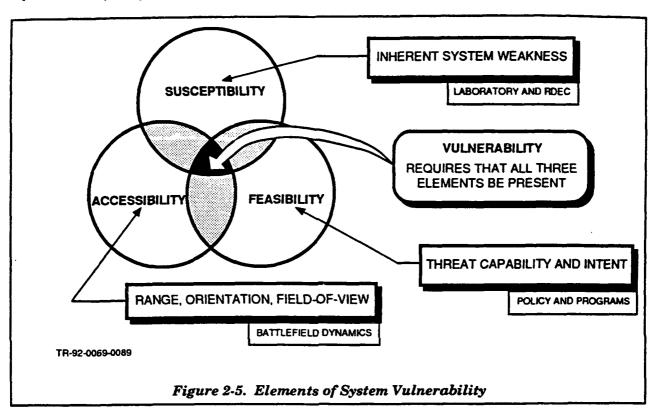
In its simplest form, system vulnerability can best be illustrated in terms of the three circles depicted by the Venn diagram in *Figure 2-5*. This diagram has been used for the past decade to clarify the elements of vulnerability and to segregate what could be done from what is likely to be done as a threat CM.

A brief explanation of each major element within the vulnerability Venn diagram is presented below

- 1. Susceptibility: An inherent characteristic within a system that can be adversely affected by some means. It can be identified and measured in a laboratory or an RDEC.
- 2. Feasibility: The scientific and engineering capability of an enemy to effectively attack a systems susceptibility and the intent to field and use this capability. The latter may reflect policy and doctrine.
- 3. Accessibility: The presence of battlefield conditions and geometry that permit an enemy to use this capability to successfully attack a system's susceptibility. Includes battle areas (forward area drone not accessible by rear area air defense), engagement geometry (soft tank belly not accessible to Dragon), or battiefield dynamics.

For any system to be considered vulnerable, it must be susceptible and accessible and the CM must be feasible. All three conditions must exist simultaneously. For example, an artillery-delivered SM may be detonated prematurely by a coarse wire mesh that is emplaced high above a threat system being protected. The effectiveness of the mesh against the SM can be measured in laboratory and field tests. However, if no known threat forces have, or plan to have, this capability, the wire mesh does not meet the criteria of feasibility against the smart weapon. Similarly, a smart weapon IR seeker that operates in the 8-to 12-µm band, filtering out other wavelengths, is not vulnerable to blinding by a low-energy laser operating

at 1.06 μ m. The far-IR seeker is not susceptible to low-energy, near-IR radiation, even though the laser and sensor may be facing one another on the battlefield (that is, the seeker is accessible to the laser). Implicit in the threats feasibility to develop a CM is his knowledge (through his intelligence) of the smart weapons systems susceptibility.



The determination of a systems EW vulnerability is made by the VAL, located at White Sands Missile Range (WSMR). The VAL has the mission of conducting independent EW vulnerability assessments of US Army weapons and C31 to hostile EW and other EM effects. VAL also has the mission to research and investigate techniques to reduce EW susceptibilities and vulnerabilities of these systems. Due to the complexity of the EW vulnerability assessment process, budget, schedules, technical design issues, and other program constraints the PM will often have to go outside of VAL to get this support. However, before the system goes before the Defense Acquisition Board (DAB), VAL will ultimately have to assess the EW vulnerability of the system. Therefore, it is advisable that VAL be appraised of ongoing EW vulnerability assessment efforts through the Survivability (CM/CCM) Test Integration Working Group (TIWG). Further, it is strongly recommended that all smart weapon PMs have an established survivability (CM/CCM) TIWG.

In support of their specific EW mission and analytical requirements, VAL has expanded the basic vulnerability diagram to include a fourth circle: interceptibility. Interceptibility highlights the adversary's target acquisition/C³I capabilities; that is, the ability to locate, identify, and engage a weapon in the operational environment in a timely manner. For example the laser repeater used to decoy a Hellfire missile must intercept and process the incoming laser designator signal in a timely manner. The EW/EM Vulnerability diagram used by VAL considers vulnerability from a more specific perspective than the three-circle Venn diagram. Both approaches have the same intent: to highlight the key factors to be considered when assessing a system's vulnerability. For consistency within this text, the more general three-circle diagram and terminology are used.

2.4.2 Survivability Considerations

Enhancing a system's battlefield survivability requires reducing that system's vulnerability. In effect, survivability can be improved by reducing one or more of the elements of vulnerability: susceptibility, accessibility, and feasibility. Protecting systems against a particular threat capability requires close cooperation between the combat and materiel developers. There must first be a determination of the existence and impact of the vulnerability before any consideration is given to a fix. Based on the vulnerability assessment, the combat and materiel developers must agree on an approach to follow in order to protect the system, or they may accept the risks or system degradation. A tradeoff analysis is essential.

The solution to making a system more survivable is not always a hardware fix. In fact, the first considerations to enhance survivability should be associated with the doctrine and tactics for employing the system, organizational changes that enhance survivability, and changes in training that enhance performance. Hardware fixes tend to be much more costly and take more time to implement. By simply changing the tactics related to the employment of a system or its position on the battlefield, the combat developer may be able to make a system more survivable.

Hardware fixes may include system hardening or design changes to make the smart weapon less susceptible (e.g., introducing filters or limiters in optical or electrical components) or less accessible [e.g., narrowing the fields-of-view (FOV) of a sensor]. Changes to protect the US system in the presence of threat CMs are generally referred to as CCMs. Feasibility can also be reduced by CCMs such as partial Faraday shielding of electronic components. This will require higher radio frequency (RF) weapon output power. The threat is less likely to field and use an RF weapon if the output power requirements stress the threat's technology.

2.4.3 <u>Assessing Cost-Effectiveness</u>

Most threat CMs can be effectively countered. It is theoretically possible (given sufficient time, available technology, funds, and near perfect intelligence information) to design and field smart weapons capable of overcoming almost all anticipated threat CMs. In some instances, the fix required may be easy

to implement and relatively inexpensive. In other instances, it may be too costly to completely protect a smart weapon against one or more threat CMs.

Tradeoffs must be made between the effectiveness and cost of implementing the CM. Providing adequate protection may require modifying important operational or technical specifications to an unacceptable cost or effectiveness level. Some CM protection and hardening approaches may after the size, weight, or sensitivity of the affected smart weapon system. Each change may impact the integration of the smart weapon with its launcher or bus, or may reduce its effectiveness during the critical endgame maneuvers. Balancing cost and effectiveness factors is the final process before deciring on the appropriate CCM to be developed or the tactics and techniques to be changed. Each smart weapons PM, working with the TRADOC proponent, must decide on a case-by-case basis how much degradation in system capability or effectiveness is acceptable in order to overcome battlefield threat CMs. The overall goal of the smart weapons developer remains to reduce the total cost per kill.

This tradeoff and risk analysis is a continuous team process that is critically dependent on the CM and smart weapon community. The agencies performing evaluations [TRADOC Analysis Command (TRAC), OPTEC, and Army Materiel Systems Analysis Activity (AMSAA)] and the agencies performing vulnerability assessments (VAL, VLAMO, and BRL) must carefully consider their impact on the requirements and technical support agencies. Whether a good system was cancelled due to incorrect or overstated CM requirements, or a bad system was fielded with significant vulnerabilities, the entire Army community losses. Intelligence analysts should be precise in their technical descriptions of threat CMs. All the uncertainty must be weighed, along with the facts, by the TRADOC proponent, the smart weapon PM, and, again, by Army decision makers.

THE CM SOLUTION PROCESS IS
A COMMUNITY EFFORT

3. COUNTERMEASURES OVERVIEW

A CM is a device, technique, or action that responds to a specific enemy action or capability; a CM is designed to reduce an enemy's capability or operational effectiveness. The purpose of a smart weapons CM is to destroy or degrade the effectiveness of the smart weapon.

3.1 COUNTERMEASURES - A DOUBLE-EDGED SWORD

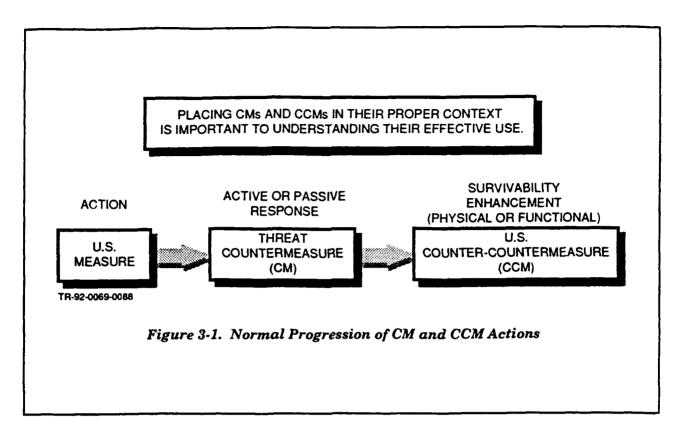
CMs are an essential ingredient of combat. Each combatant on the battlefield will try to counter the weapon systems of the other side. In most instances, CMs have been identified and their employment planned for prior to combat. They are then adjusted during the battle based on their observed effectiveness.

In planning for the use of CMs, it is important to consider not only the friendly CMs, which are designed to reduce threat capability, but also the threat CMs being used against your own weapon systems. The devices, techniques, or actions taken to respond to threat CMs are CCMs. CCMs are devices, techniques, or actions designed to permit a system to function effectively even in the presence of threat CMs. CCM design changes are typically referred to as system hardening.

When a new weapon system concept is first envisioned, it is a routine matter to consider the potential or known threat CM that may be directed against the system to defeat or degrade it. In these early developmental stages, the first friendly CCMs are incorporated into the systems design and planned for in its operational employment. CM solution planning is continuous in the RDT&E system. The earlier vulnerabilities are identified, quantified, and specified, the more likely that cost-effective CCMs can be developed.

The normal progression of CM and CCM actions is shown in *Figure 3-1*. The context in which the terms CM and CCM are used is important in understanding their intent. Confusion can occur when the parallel threat capability, US CMs, and threat CCMs are discussed. Within this guide, CM refers to a threat CM against a US smart weapon unless clearly noted otherwise.

As depicted in the *Figure 3-1*, CMs degrade a smart weapon's capability, whereas CCMs allow the smart weapon to function in a CM environment or induce the adversary to not field the potential CM. Some CCMs do not fully negate or eliminate a threat capability to employ CMs, but only reduce the CM's effect on a system. In other examples, CCMs do fully negate the CM or affect the threat capability to employ CMs.



3.1.1 Classes of CMs

CMs can be grouped in several different ways. For this study and the overview chart (Appendix D), they have been grouped by class based on their function related to smart weapon sensors. These classes are identified in *Table 3-1*.

The terms threat, responsive, and reactive are often misapplied when associated with CMs. From the definition presented in this volume, a CM is a device, technique, or action. A threat is a force, country, or political entity that possess a means, motive, and will to harm US forces. In simple terms, the threat can be viewed as the enemy. The determination of the threat to a system is made by the appropriate Foreign Intelligence Office (FIO) or FID and is documented in the STAR. Threat CMs are those devices, techniques, or actions used by the threat to degrade the system's performance. As stated earlier, this study is primarily focused on threat CMs. A responsive threat CM is a CM developed/fielded by the threat to defeat a specific weapon system. It may have an impact on other systems, but the threat developed (or will develop) the CM in response to the particular weapon system in question.

Table 3-1. Classes of EW CMs to Smart Weapon Sensors

CLASSES	EXAMPLES OF CM USE		
Signature Alteration	Foliage Camouflage paints and nets Redirected engine exhausts Hot-spot masking RAM	TACTIO	
Decoys/ Deception	Repeaters Mockups and Replicas Heated plates and flares Reflective chaff Corner cubes Phosphorous smoke	00 420	
Obscurants	Smoke Fog oil Dust Burning oil Chaff (absorptive and reflective)	H E C H Z -	
DEWs/ Jammers/ Semi	Lasers (low and high energy) RF emitters High-powered microwave Hot-spot beacons	Q D E Ø	

Normally, a responsive CM is fielded after the initial operation capability (IOC) of the US smart weapon system. However, it is possibly through poor operational security plans that sufficient technical information on the smart weapon is leaked to a foreign power. If this occurs, a responsive CM is fielded by a threat prior to the smart weapon system fielding. Examples of a responsive CM would be the introduction of acoustic decoys in response to a smart weapon that used acoustic sensors for target detection. Not all CMs faced by a smart weapon system are responsive CMs. There are CMs used by the threat as a standard part of tactics and doctrine. A CM that is responsive to another weapon system may have a degrading impact on the smart weapon of interest. These CMs are designated baseline CMs, as they are part of the ever-present dirty battlefield environment. An example of a baseline CM is the use of hull defilade fighting or firing positions. As a tactic, hull defilade was in use long before smart weapons were introduced on the battlefield. The original intent was to avoid detection by threat weapons and to offer ballistic protection. Although this CM was not intended for smart weapons, it could have a significant detrimental impact on the performance of certain smart weapons.

Threat CMs to a particular smart weapon system are either baseline CMs or responsive CMs. This division between baseline and responsive threat CMs is being introduced by AMC-SWMO to better clarify the issues of CM effectiveness on smart weapons. In an across-the-board review of smart weapon threat CMs, the baseline CMs should be addressed in all smart weapon system survivability annexes. Their

descriptions, employment method, and occurrence on the battlefield should be consistent from annex to annex. If a smart weapon system is unaffected by a baseline CM, it should be so stated, and the CM ignored in the design and development process. The notion of baseline CMs also places a requirement on the entire Army community to develop a survivability annex that includes all baseline CMs. This would greatly aid the smart weapon development process by having common standards of baseline CMs. Hull defilade should have the same description in all annexes. The affect of hull defilade on the smart weapon will naturally be different from smart weapon system to smart weapon system. The important point is that the difference is a result of the smart weapon system design and operation, not the definition of hull defilade.

Reactive CMs are those that must predict or detect an activity (e.g., an incoming smart submunition), then initiate an effect (e.g., initiate radio frequency (RF) jamming or pop smoke). Reactive CMs are initiated during the smart weapon engagement. Thus, countering reactive CMs can be achieved by reducing the threat's ability to perceive the triggering action.

3.1.2 <u>Categories of CMs</u>

Threat CMs that a new US system may encounter on the battlefield are designated as belonging to specific CM categories. There are three threat CM categories and each is identified based on the probability of occurrence of the CM on the battlefield and the approval of the CM by DCSINT. A CM assignment to a category should not change for different types of smart weapons. An exception would be in the case of widely different planned fielding times. Criteria established for each category are provided in *Table 3-2*. A brief explanation of each threat CM category follows.

- 1. Category I, labeled a Routine CM, is officially acknowledged as having a high probability of occurrence on the battlefield. It will be encountered by the smart weapon in its normal operation. The CM may be a standalone device or system, or may be incorporated into the design of the threat systems. These "built-ins" are designed to enhance the effectiveness of the threat system against a broad range of anticipated US systems (e.g., smoke on tanks). Smart weapon system designs are expected to meet specified performance levels for this CM, in the first production.
- 2. Category II is designated a Less Frequent CM. It is officially acknowledged by the intelligence community as having a low to medium probability of being encountered. A Category II CM could be an extension of or a higher intensity variant of a Category I CM (e.g., a very thick smoke, or a weapon variant of a laser designator or RF source). System design implications are similar to those for Category I, except that performance-level maintenance may not be as stringent as for Category I, but are still required in the first production run.
- Category III is designated a Potential CM. It is considered to be technically and tactically feasible but is not approved by the intelligence community (DCSINT). An example of a CM that falls into this category is a US CM capability not observed in threat research and development (R&D). System implication is less stringent. A pre-planned product

improvement (P³I) program may satisfy CM planning requirements. Some level of performance may be required in the first production run.

Table 3-2. Categories of Threat CMs

CM Cate;jory	Criteria	
I - Routine	DCSINT approved High probability of encounter	
II - Less Frequent	DCSINT approved Low to medium probability of encounte	
III - Potential	Technically and tactically feasible Not DCSINT approved	

3.2 CM EFFECTS AND EMPLOYMENT

Whenever a US weapon system is built and fielded, a potential enemy would like to reduce the effectiveness of that system. Improvements or capabilities to reduce the effectiveness of specific weapons frequently take the form of responsive CMs. Responsive CMs include chaff or electronic jamming against set bands of RF smart weapons or improved flares against IR sensors on smart weapons. Some CMs are simply fine tuning of existing CMs (broader spectral band blocking in smokes).

3.2.1 CM Effects and CCM Reaction

Paints have been used as a CM to reduce the visual detectability of targets for many years. Paints can minimize the reflection from the sun and decrease the contrast with the background. Combat vehicles are usually painted with a camouflage design to reduce their visibility. Efforts have also been made to reduce the IR radiation from the hot areas around the engine exhaust on helicopters and tanks as a CM against IR guided missiles. Altering hot spots can also degrade smart weapon aimpoint selection, thus lethality.

Stealth is one of the more recent developments in the area of CMs that has received considerable publicity. The idea of stealth is to make an attacking airplane or missile less likely to be detected by enemy radar by reducing its radar cross section (RCS) through special shaping, the use of radar absorbing coatings, and/or the employment of nonconductive materials in its construction. This is not an easy task, since radars operate at many different frequencies and RCS is dependent on frequency. Radar detection range is also a function of the fourth root of the RCS, (RCS)^{0.25}. In other words, the cross section must be reduced by a factor of 16 for each halving of the detection range. Stealth technology was specifically developed as a CM to avoid acquisition by radar systems. Stealth techniques and technologies are now being applied across the electro-magnetic spectrum, and even in the acoustic and seismic regions to lower

the detectability of the weapon system from the threat. Applied to the smart weapon, it is a potential CCM to preclude a reactive CM from being deployed once detection of the incoming submunition is accomplished.

When a CM is developed by an enemy to reduce the hit or kill probability of a smart weapon, methods are sought to defeat the CM. These new efforts often take the form of CCMs. Electronic counter-countermeasures (ECCMs) may be employed to reduce the impact of jamming on RF smart weapons. A dual-color or dual-mode IR smart weapon may be developed to defeat flares. A new warhead may be designed to defeat new armor. *Table 3-3* portrays a typical series of actions and reactions (CM and CCM) to the use of smart weapons.

Table 3-3. Samples of CM/CCM Reactions to Smart Weapons Designs

Smart Weapons Design	Possible CM Response	Possible CCM Respanse
RF Seeker	Chaff	Longer wavelength seeker
IR Seeker	Flare	Dual-color seeker
Hot Spot Tracker	Alter signature	Image/feature tracker

3.2.2 Range of CM Effects

The effects that can be achieved on a smart weapon system by threat CMs cover the spectrum from temporary degradation to catastrophic kill. Each potential threat CM must be examined as it relates to each component of a smart weapon system or the system as a whole. An extensive data base of CM effects is available from several Government agencies including VAL, SMO, and the Center for Night Vision and Electro-Optics (CNVEO).

Whether increased or decreased, altering a target's signature may cause a smart weapon not to recognize the resulting image. The intended target may blend into the background. Decoys, like a tank mockup or a flare, present characteristic target signature information to a smart weapon that may divert attention from the real target. Obscurants, such as smoke or fog oil, may screen the target from the smart weapons seeker so that the target cannot be seen. Each of these CMs has the effect of concealing or diverting attention away from the real target.

DEWs are a family of weapons consisting of systems that use the energy within the EM spectrum as their primary kill mechanism. The DEW family includes lasers, RF emitters, and particle-beam weapons. Particle beams will not be considered in this study due to the limited feasibility of their being fielded and employed tactically. DEWs are active CM weapons in that they degrade or blind the smart weapon seeker or disrupt onboard electronic signal and data processing (to include warhead fuzing). It may be possible to

activate an electronic fuze and prematurely detonate the smart weapon warhead using an appropriate external CM source, such as a high-powered microwave (HPM).

A sample of the types of effects that can be achieved by a DEW CM on specific materials and target components is shown in *Table 3-4*. The DEW CMs considered in *Table 3-4* include high- and low-energy lasers (HEL/LEL), and HPMs. The effects identified must be quantified and as sessed as they apply to the components and subsystems of the smart weapon system under investigation. Effects will vary based on several factors, to include DEW system power, range to target, atmospheric conditions, and specific materials that make up the target system.

Table 3-4. Typical Effects from DEWs

160te 5-4. Typical Effects from DEWs				
DEWs		Targets	Typical Effects	
HE		Aircraft/helicopter canopies Thin-skinned vehicles Optics Vehicle vision blocks	Fogging/flash Burn-through Crazing/cranking Crazing	
Lasers	Optical sensors Missile seekers EL Bio-optics Pilots Gunners/gun crews	Saturation Detector burnout Vision degrade/damage Temporary blinding Hemorrhagic lesions		
HPM Electrical systems Electronic components Integrated circuits Sensitive chips Weapon fuses G&C systems		Electronic components Integrated circuits Sensitive chips Weapon fuses	Electronic upset/jam Disrupt or negate Saturation Burnout Fuse activation Break track	

Once a smart weapon component and subsystem effects are understood and measured, the impact on the system can be assessed. The results can be validated through laboratory or field testing. If realistic system testing is impractical, simulations of the CM engagement should be considered as a viable alternative.

3.2.3 <u>Tactics, Techniques, and Procedures</u>

As indicated in *Table 3-1*, CMs that cross all functional types are the tactics, techniques and procedures used by the threat to reduce weapon system effectiveness. Tactics, techniques, and procedures used as CMs against smart weapons may include such actions as dispersion during road march to reduce target densities or maximum use of natural terrain features to reduce the clear LOS opportunities needed by direct-fire GMs. A common and specific tactic is the use of defilade positions. The use of defilade positions is generally standard and quantifiable in terms of its probability of occurrence and effect on smart weapon performance.

Figure 3-2 shows four types of defilade positions. Although these are all common in terms of their descriptions with respect to smart weapons, their effect on smart weapons will vary with each system. The hull-down posture shown in Figure 3-2 is a tactic used by armor when either attacking on defending. To the extent practical, the technique is to fire from behind a berm or rise in the terrain such that only the turret of the tank is exposed to the enemy positions. From the rear, side, or top perspective, the tank may appear to be out in the open. However, from the perspective of the GM firing position, only the turret is exposed. This type of hull-down posture is only effective against an acquisition sensor of a direct-fire GM. The tank may also occupy a turret-down position in which only the tank commander can observe the battlefield. The cannon is shielded by the terrain and cannot fire. The third position shown in the figure addresses the case in which the threat armor has quickly dug itself into a self-prepared position. In this case, only minimal ballistic protection and signature alteration is achieved. The dug-in fighting position shown in the figure reflects the case where the enemy has had sufficient time and resources to prepare fighting positions. Although the hull may be covered, freedom of movement and clear observation for the turret should be maintained. These positions generally offer signature alteration from all aspects and at times from the top. The latter is also true for those SMs with active sensors that use target/range background and/or size profiling to detect the target.

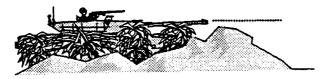
When considering the effect of defilade positions on smart weapon effectiveness, three points must be addressed: the type (see *Figure 3-2*), the occurrence on the battlefield, and the perspective of the target from the smart weapon seeker. The point concerning the perspective of the target from the perspective of the smart weapon seeker warrants further explanation. In the hull-down or turret-down posture, the impact is primarily on the direct-fire GM acquisition sensor located forward of the enemy position. As the GM or SM flies over the dug-in position, the scene is quite different. What the smart weapon sees is the top of a tank or self-propelled howitzer sitting in a hole (or out in the open in the case of the offensive hull defilade posture). From this top- looking perspective, several important factors may increase or decrease the performance of the smart weapon. In the case of the prepared positions, the disruption of the soil around the position may change the background signature for both the passive and



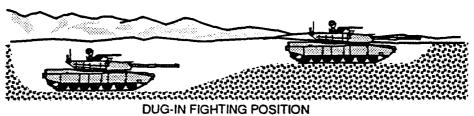
HULL DOWN POSITION (CAN FIRE CANNON)



TURRET DOWN POSITION (COMMANDER CAN SEE, CAN'T FIRE CANNON)



SELF-PREPARED POSITION (PREPARED BY ORGANIC ASSETS



(PREPARED BY ENGINEERS)

TR-92-0069-0090

Figure 3-2. Defilade Positions

active sensors. The impact (positive or negative) to target detection depends on the system and the nature of the soil excavation. In the case of a defensive position, the distinction between target and background may be harder to discern. Hot features detected by an imaging IR seeker may in fact be the side of the position that has been heated by hot exhaust blowing on it. Active sensor [laser radars and millimeter wave (MMW)] that use range imaging and profile techniques may be severally affected as the target is buried more in the ground. Defilade is an important CM that must be addressed by smart weapons developers.

3.3 BATTLEFIELD EMPLOYMENT OPPORTUNITIES

The success of smart weapons in the recent Middle East conflict has focused attention on the capabilities of all smart weapon systems. The accuracy of the many different smart weapons used in Desert Storm will accelerate and expand their development and use. The increased use of smart weapons will inevitably be accompanied by the development of more sophisticated CMs. Threat CMs to smart weapons will grow correspondingly and be closely associated with the targets that smart weapons attack.

Many types of CMs, active and passive, are used by potential adversaries in protecting systems on the battlefield. The full range of CM options available to the threat should be assessed to determine the most cost-effective approach to enhancing the survivability or mission effectiveness of smart weapon systems. It is important to recognize that the ultimate function of a smart weapon is to destroy a specific threat target. Consequently, most CCMs used with smart weapons are designed to enhance the functions of target attack and mission accomplishment. The physical survivability of an individual smart weapon is specifically not an issue. The ability of an HPM to physically damage enough SMs from a single carrier such that only minimal damage from the SM attack is achieved is, of course, a concern. The point is that the effectiveness of the SMs is important, not their individual survivability.

4. COUNTERMEASURE EFFECTS ON SMART WEAPONS

The following sections discuss the effects of CMs on smart weapon systems and is written from a vehicle survivability standpoint. *Figure 4-1* provides a synopsis of the effects of these techniques. The type of CM, its effective spectral band, and the smart weapon function degradation are displayed. Section 4 is intended to introduce the technical issues and provide insights to CM techniques and devices that may affect smart weapon systems. There are three objectives to this section: 1) provide technical descriptions of the CM and the generic effect on the smart weapon; 2) describe the technical data that is necessary to fully characterize the CM; and 3) to provide references to models and databases that contain the specific technical details necessary to characterize the CM. The third objective is backed up by Appendix C "Resource Organizations" of this volume. For more detailed discussions on the impact of these CMs on smart weapon technologies, refer to Volume II of this series. The section is organized into CM classes. Each class is broken down further into the spectral bands of interest. Some CM classes are applicable to more than one spectral band. These classes are discussed according to the band in which they are most common.

4.1 SIGNATURE ALTERATION

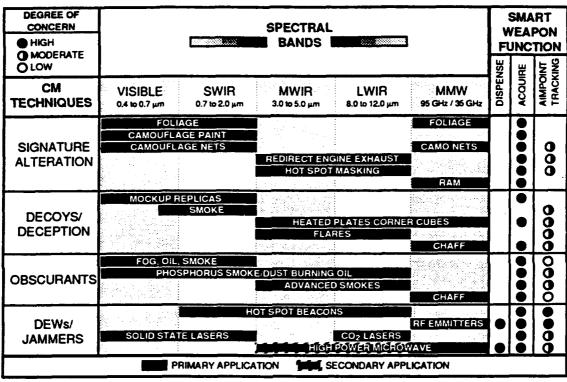
Before discussing SIGNATURE ALTERATION, the notion of SIGNATURE REDUCTION is introduced. SIGNATURE REDUCTION refers to the signature level attained through the basic design of the vehicle.

SIGNATURE ALTERATION as a CM uses the modification, suppression, and augmentation of the measurable target features to prevent or degrade acquisition and aimpoint tracking by smart weapons. The objective of signature alteration is to make the target look like the background.

The following are definitions of the different approaches to altering vehicle signatures. These approaches are defined in terms of the sequence in which they might occur or, more specifically, the initial definition is that associated with the base vehicle signature from which all alterations will be made. *The emphasis in this report is SIGNATURE ALTERATION*. The following are definitions of methods of SIGNATURE ALTERATION:

SIGNATURE MODIFICATION: The use of devices that mask key features of the vehicle from the seeker. The total energy emitted by the vehicle remains constant; however, it is modified, diverted/redirected in such a manner that the modified signature results in a reduced probability of detection or hit.

SIGNATURE SUPPRESSION: The use of devices (nets, RAM, foliage, etc.) to lower vehicle signature. Signature suppression causes a decrease in the total energy emitted by the vehicle and therefore received by the sensor. Signature suppression causes a decrease in the probabilities of acquisition and hit.



TR-91-0069-2526 UNCLASSIFIED

Figure 4-1. (U) Relative Impact of CM Types

SIGNATURE AUGMENTATION: The use of devices that increase the signature of the vehicle by increasing the total energy emitted. Techniques to accomplish this may be similar to those used for signature modification, except that the total energy of the vehicle is increased. This results in a decrease in the prominence of key features that support aimpoint selection, therefore decreasing the probability of hit at the expense of increasing the probability of acquisition.

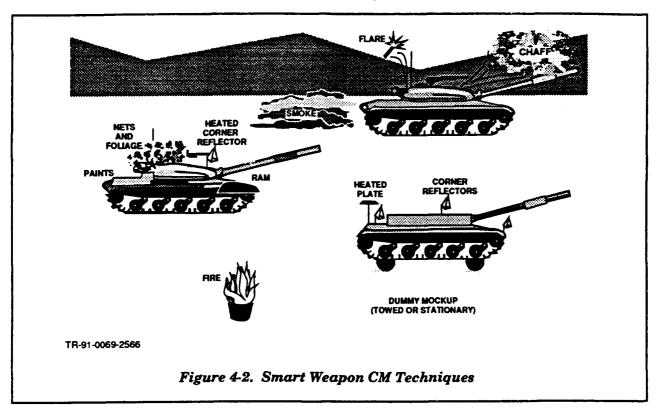
For an IR system, the differential temperature and surface emissivity of the target must be altered to more nearly match the background temperature, or the temperature of hot spots must be reduced to resemble the temperature of the remainder of the target. To alter the MMW signature, the magnitude and characteristics (e.g., polarization) of the target reflectivity must be modified to match the background. This is accomplished by masking the engine inlets (aircraft targets), joints, abrupt transitions, and areas of little curvature or changing target surface texture. In addition, the shape of the target can be modified to change the MMW reflectivity. Usually, signature alteration of typical targets involves reducing the MMW reflectivity. However, there are instances when increasing a target's signature (IR, MMW, active or passive) so that it blends into the naturally reflective background is appropriate. For both IR and MMW systems, signature alteration CM techniques can be enhanced by the use of decoys. The two techniques are complementary, so their combined use should be considered.

The acquire and hit functions of smart weapons are affected by the application of electro-optic (EO)/IR/MMW signature alteration techniques. The acquire function is affected if the overall signature is suppressed, and the hit function is changed if the "signature" is rearranged/altered thus affecting aimpoint selection. To adequately model the effects of these techniques, the amount of signature alteration expected must be specified, either as a percentage change in differential temperature or as a change in decibel received. If available, a more precise characterization of the altered target signature is to specify the absolute signature level achieved with the signature alteration technique. For force effectiveness and many-on-many modeling, the reduction in footprint, probability of acquisition (P_{acq}), or range as appropriate must be specified.

There are two parameters that characterize the performance of the acquisition function, P_{acq} , and the false alarm rate (FAR). For a given detectable signature and background clutter, high P_{acq} can be traded off against high FAR and vice-versa¹. Since both are important to system performance, both the impact on P_{acq} due to a signature alteration technique and the associated FAR must be known. Oftentimes, system P_{acq} will be measured and reported for a variety of IR kits, radar absorbing material (RAM), and other signature-reduction techniques. However, without the simultaneous FAR that was maintained, the data are of little value.

¹"Burle Electro-Optics Handbook," Burle Technologies, FOH-11, 1974.

Some common methods that after the signature of the target are: camouflage nets, foliage, camouflage paint, redirecting engine exhaust, hot spot masking, and RAM. Foliage, camouflage paint, and camouflage nets are primarily effective in the visible and short-wave infrared (SWIR) spectral bands. The techniques of redirecting engine exhaust and masking hot spots are effective mid-wave infrared (MWIR) and long-wave infrared (LWIR) CMs. RAM is used as a CM for radar systems. The impact of foliage and nets on IR and MMW systems generally has been overstated. An example is in the case of IR signatures. Depending on weather conditions and types of foliage/nets used, the effect on the target signature can range from very effective to that of enhancing the target signature. For MMW systems, an entirely new set of issues is raised. The general trend is that foliage will tend to significantly lower the RCS of the vehicles. Figure 4-2 depicts a scenario of these techniques. For more details on nets and foliage, the reader is strongly encouraged to review the data presented on this subject in Volume II of this series, "Effects of Countermeasures on Smart Weapon Technologies," January 1992.



4.1.1 <u>Visual Signature Alteration</u>

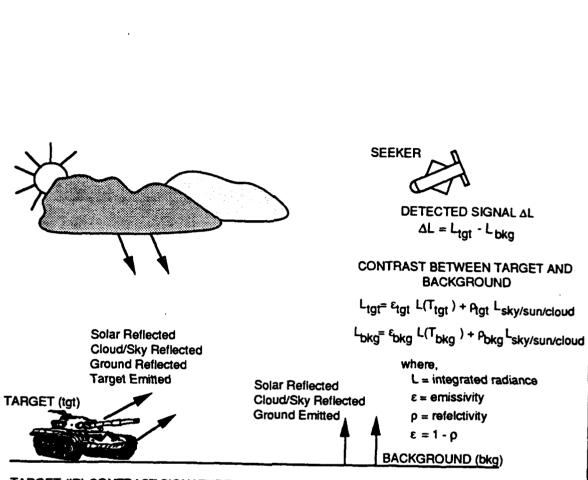
Visible signature alteration techniques attempt to disguise the target. Camouflage nets and foliage mask the shape of the target in an attempt to blend the target into the background. Targets are painted to match the environment, e.g., tanks in the Middle East are painted in the desert sand camouflage

pattern rather than the green hues of a forest. A possible CM technique is to paint vehicles with a paint that has low reflectivity in a spectral band of concern. To counter the laser designators that operate at 1.06 µm, a paint with low reflectivity at this wavelength could be applied to vehicles. However, one problem exists with this tactic. Vegetation exhibits high reflectivity at SWIR, including 1.06 µm (the chlorophyll band). If an active SWIR system is used to view the vehicle, the vehicle would appear as a black hole (low reflectivity) in a white background (high reflectivity).

4.1.2 <u>IR Signature Alteration</u>

Nonimaging IR signature alteration techniques involve thermal management. The pertinent signature is the difference between the radiated power of the target and the radiated power of the background. This difference can be expressed in terms of the emissivity area ΔT or $\epsilon A(\Delta T)$ product, where ε is the emissivity, A is the target area, and ΔT is the target-background temperature difference. A target with twice the area and half the temperature difference has the same IR signature as a target with half the area and twice the temperature difference. These two targets appear the same to a nonimaging (point source) sensor, where the target area is always less than the instantaneous field-of-view (IFOV). Figure 4-3 shows the sources of IR radiation usually present. See Appendix B: Definitions and Acronyms for an explanation of the symbols shown. As shown in the figure, sensed IR energy can be a result of reflection from the sun or sky rather than actual thermal radiation from the target. The latter usually dominates. Techniques, such as camouflage nets and foliage, which mask the general shape and reflectivity of the target, reduce the thermal signature by making the target resemble the background. Under some conditions, these techniques have little effect on the IR signature. Paint is also used to mask the general shape and reflectivity of the target by redistributing the thermal energy both spatially and spectrally. Ideally, the paint lowers the emissivity of the target and reduces the thermal emissions. This can be very effective on small hot regions (like an exhaust pipe). The heat radiated with the lower emissivity is removed by conduction and convection. In general, the laws of thermodynamics do not allow total freedom in reducing all aspects of a given thermal signature. Energy must be conserved, the heat must go some where. These thermal signature alteration techniques mainly affect the target acquisition process.

Another IR signature alteration technique affects the terminal guidance process by shifting the smart weapon's aimpoint. The sophistication of aimpoint selection and tracking has matured far beyond the simple tracking of the centroid of the hottest spot on the vehicle. Aimpoint selection and tracking algorithms used by Javelin and Bat will use target features (hot and warm spots) and target edges and shape. As an example, an algorithm may shift the aimpoint from the hottest spot (exhaust on the side of the tank). The aimpoint shift vector (direction and distance) would be the average of the vector from the exhaust to the center of the target and the vector from the exhaust to the center of the target hot spots. Methods used to defeat aimpoint selection are redirecting engine exhaust and masking hot spots. These techniques can



TARGET (IR) CONTRAST SIGNATURE IS A FUNCTION OF BOTH EMITTED AND REFLECTED ENERGY. REDUCING THE EMITTED COMPONENT WILL INCREASE THE REFLECTED COMPONENT.

TR-91-0069-2567

Figure 4-3. IR Emissivity and Reflectivity

alter the location of the target's hottest spot. This shift in hot spot location will cause a change in the smart weapon's aimpoint selection. Also, as the smart munition closes in on the target, the signature could change; instead of one large hot spot, there could be a grouping of several hot spots. This change in signature has an effect on the aimpoint tracking of the missile, which can cause a miss.

The term signature alteration/reduction has different meanings depending on the sensor being used and the target attributes it is detecting. For example, the forward-looking IR (FLIR) used by the human operator, such as the Javelin Command Launch Unit, detects a modulated signature. In this case, it is insufficient to characterize the signature alteration as a lowering of the average thermal contrast given by:

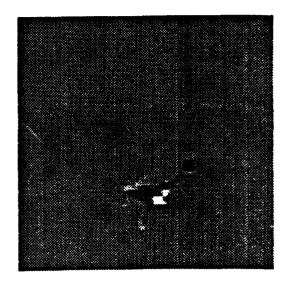
$$\Delta T_{\text{standard}} = |T_{\text{tgt}} - T_{\text{background}}|$$

where, T_{tgt} is the average target temperature and $T_{background}$ is the average background temperature. In the case of FLIRs, the correct definition for the signature is

$$\Delta T_{\text{enhanced}} = \sqrt{((T_{\text{tgt}} - T_{\text{background}})^2 + \sigma_{\text{tgt}}^2)}$$

where, σ_{tot} is the standard deviation of the target temperature as it is displayed by the FLIR. To reduce the target's signature, one must also reduce the standard deviation of the target's temperature, not just the target-background difference. Figure 4-4 demonstrates this effect. This figure shows two LWIR images of a small experimental aircraft (Long-EZ). The view is a rear aspect, with the Long-EZ's rear-mounted propeller and engine clearly visible. This area appears hot to the IR sensor; however, the cowling and wingtips appear cold. As a result, the average temperature of the target closely matches that of the background. Use of the standard ΔT definition predicts that the target cannot be seen; however, a more accurate prediction is reached by using the enhanced ΔT definition, given above ($\Delta T_{enhanced}$). The variability of temperature on the target results in a high value of σ_{tot} and leads to a higher ΔT value. For the image on the left, $\Delta T_{standard} = 0.026$ K and $\Delta T_{enhanced} = 0.207$ K. For the image on the right, the background has been modified to be uniform and at the mean temperature of the target. For this image, $\Delta T_{standard}$ = 0.000 K and $\Delta T_{enhanced} = 0.206$ K. Since the target image on the right can still be detected, the use of the ΔT_{standard} is inappropriate as it would predict 0% probability of detection (or recognition for that matter). For the camera system used, the $\Delta T_{enhanced}$ predicts a near unity probability of detection, and therefore is a better representation of the Long-EZ's detectable signature. For high-resolution IR imagers, it is important to reduce temperature variability as well as the average temperature difference between the target and the background.





TR-92-D069-1008

Figure 4-4. ΔT Definitions

4.1.3 MMW Signature Alteration

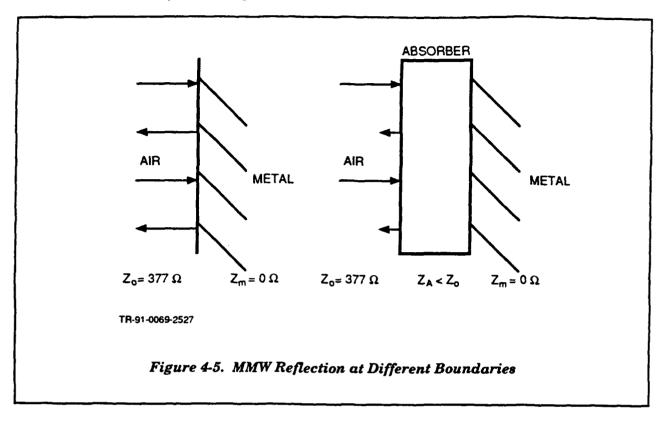
RAMs are designed to absorb incident radar signals to reduce the RCS of the coated object. These absorbers are produced by altering the magnetic (permeability, μ) and dielectric (permittivity, ϵ) properties of existing materials. The factors governing the reflection (R) of a signal are the impedances (Z) of the media through which the wave propagates and the surface (metal) impedance. The equations for impedance and reflection are given below.

$$Z = (\mu/\epsilon)^{1/2}$$

$$R = -(Z_{air} - Z_{metal})/(Z_{air} + Z_{metal})$$

When an EM wave strikes an air-metal interface, total reflection (R = -1) occurs since the metal acts as a short circuit (μ = 1 and ϵ = ∞) to the incident signal. The negative value for R indicates that at the air-metal interface, the reflected wave is 180° out of phase from the incident wave. The noncoherent reflected energy is just the absolute value |R|. By placing a material between the air and metal, the reflectivity can be controlled by altering the impedance at the interface. Complete absorption (R = 0) is achieved when μ = ϵ ;

however, μ never approaches the magnitude of ϵ over a useful, broad frequency range. Consequently, some reflection will always occur. *Figure 4-5* shows the reflection at a surface coated with a RAM.



The composition of RAM determines which polarizations will be attenuated. If the addition of RAM only reduces one polarization of the radar signal, the target can still be detected because of the existence of the other polarization. Because of the polarization discrimination ability of smart weapons, RAM is more effective if it reduces the radar return in all polarizations.

4.2 DECOY/DECEPTION

A decoy is a CM technique that utilizes false targets to deceive the smart munition into thinking the decoy is the intended target. The decoy attempts to duplicate the signature of a target as it appears to sensors. This may include matching the reflected signal (σ_{RCS} or ΔT) or the signature characteristics (distribution of scatterers, size, shape, etc.). The smart weapon may expend some of its acquisition and tracking time and munitions on the decoys, thereby allowing the real targets to elude the enemy. These false targets can alter the acquisition and hit probabilities of the smart weapon. *Figure 4-2* contains examples of decoys in the battlefield environment. The false targets include corner cube reflectors, flares, fires, heated plates, and thermally generated smokes (such as white phosphorus or smoke from petroleum fires).

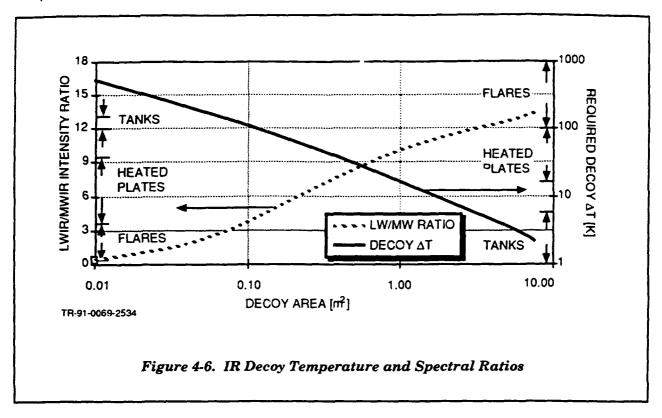
Decoys may be modeled if the type of decoy is specified. For example, the corner cube type (two-sided or three-sided) and location relative to the target must be provided. Flares must be specified by their material, temperature, spectral band, intensity, placement, and duration. Fires should be defined by their temperature and the material being burned. The temperature and material must be specified for the thermally generated smoke. For this particular CM, the atmospheric conditions, such as wind speed and direction, must also be considered.

4.2.1 Visual and IR Decoys

Flares, fires, heated plates, and thermally generated smokes are potential decoys for IR systems. These CMs provide additional targets that must be tracked. Flares and fires provide a hot spot, which may or may not match the characteristics of the target being protected. Depending on the type of IR system, the position of the flare or fire in the FOV, and the temperature of the CM, the sensor may acquire and track the decoy. If the smoke is hot enough, the system may lock-on and track the edge of the smoke cloud resulting in difficulties with acquisition and hit. Heated plates provide another way to counter some IR systems. Ideally, the heated plate must not exceed the temperature of a typical target or the sensor's two color discrimination logic could reject it as a viable target. (This assumes a two color IR sensor.) With solar loading, it can be hard to control the temperature of these plates. Smoke and flares are examples of reactive decoys. In a reactive scenario, these CMs are dispensed once an incoming smart munition is detected. The target vehicle can throw flares or launch chaff or smoke to confuse the incoming smart munition.

The function of an IR decoy is to generate the equivalent amount of emitted IR energy used by the smart weapon to detect the real target. The IR decoy needs to be inexpensive and carried in quantity in order to be cost effective and tactically practical. For the IR decoy to emit a specified in-band intensity, it can be either very small and very hot or very large and warm. Flares are typical of the former and heated plates of the latter. The IR smart weapon CCM of choice is a two-color system. Other IR CCMs are based on image processing where the size and shape of the target are used for discrimination. Although two-color seeker designs have not always met expectations, they still remain very popular. In a two-color system, each point in the scene is measured in two spectral bands. The ratio of the signals in the two spectral bands is a measure of the surface temperature of the scene. Figure 4-6 illustrates this point for nonimaging point source detection. The decoy is designed to emit 10 W/sr of energy in the LWIR band. This is roughly equivalent to a 2.3- by 3.2-m tank at a ΔT of 2°K, with a 290°K background temperature. Against a singlecolor, ponimaging, LWIR seeker, the decoy can operate effectively if it has the appropriate ΔT for the given decoy surface area as shown on the right side of Figure 4-6 and the curve marked "Decoy \(\Delta T". \) A two-color sensor using 8 to 12 and 3 to 5 µm can negate the effect of the decoy by measuring the LWIR/MWIR intensity ratio. This measurement is shown on the left side of the graph. Flares will have very high ratios, heated plates lower, and tanks and other targets will have the smallest ratios. The point of Figure 4-6 is to

demonstrate that the more attributes used by the smart weapons nensor to detect the target (i.e., intensity, temperature/color ratio, size) the more the decoy must look like the real target in order to be effective.



The use of smokes to generate decoys is most effective against GMs that use a visible or SWIR laser to designate the aimpoint on the target. By using a smoke that is a strong scatterer at these wavelengths, the strongest signal detectable by the guided munition will be the reflection of the laser designator off the smoke cloud and not the target. Smoke deployed between the target and laser designator (not the missile) will have two beneficial CM effects. First, little laser radiation will reach the target to be reflected, and second, a spot will form on the leading surface of the smoke cloud. The missile would thus track the smoke and not the target. The effects and characteristics of smoke will be further discussed in Subsection 4.3.1.

4.2.2 MMW Decoys

Corner reflectors, Luneberg lens reflectors, chaff, repeaters, and vehicle mockups are used as decoys for MMW systems. These false targets employ some form of radar target size augmentation to fool enemy radars. They provide another target to be engaged. Corner cube reflectors are mutually perpendicular planes that reflect nearly all the incident radiation back along its path. When offset from the target by a few meters, the hit probability on the real target could be reduced.

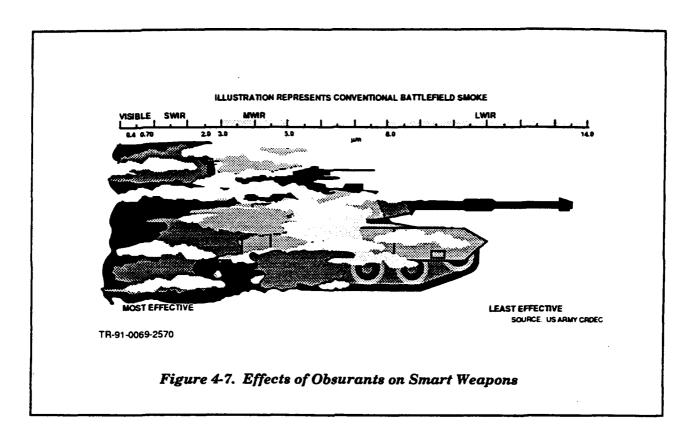
Chaff can be used as a decoy for self-protection measures. For chaff to be optimally effective as a decoy, a means for detecting the incoming missile is necessary. A bloom of chaff is launched upon detection of an incoming missile in hopes that the target lock will be transferred to the chaff. Also, since the velocity of the cloud drops to zero and Doppler radar can distinguish between a chaff cloud and a moving vehicle, chaff is a more effective CM for stationary vehicles.

Corner cubes and EO/IR retroreflectors exist for visible, SWIR, MWIR, and LWIR active sensors. Due to the characteristically narrow beam of the laser designator, the narrow acceptance angle of the retroreflector and the relatively high cost of these CMs, they are impractical as decoys to conventional smart weapons. Further, unlike MMW decoys, they would not be classified as field expedient due to the high degree of optical tolerances required to manufacture them.

Besides the conventional decoys, there is battlefield clutter and field expedient CMs that may behave as decoys. The battlefield environment provides some MMW and IR decoys. Dead hulks, burning hulks, and tires scattered on the battlefield are effective decoys. Dead hulks can deceive MMW systems because they are metallic and reflect radar signals. Dead hulks and tires are IR system decoys since they heat up due to solar loading. For tires, the combination of emissivity and thermal mass (thick rubber) creates a hot source when exposed to direct sunlight. Some decoys can be used against both IR and MMW systems. To be effective in both regions, such decoys must exhibit significant thermal and radar signatures. Burning hulks are decoys for both systems; the fire creates a thermal signature and the hulk reflects radar just as other targets. Another example of a combined decoy is a heated corner cube reflector. These false targets may lure smart weapons away from real targets. In addition, field expedient CMs can be constructed from the battlefield and natural clutter to form decoys. Reference is made to Volume II of this series, "Effects of Countermeasures on Smart Weapon Technologies," January 1992, for a discussion of classified decoy data.

4.3 OBSCURANTS

Obscurants are materials that are interposed in the propagation path of sensors. An obscurant attenuates the target signals through scattering and absorption phenomena. It does not alter or suppress the target signature, but rather reduces the amount of energy reaching the sensor (or munition in flight) from the target; that is, it changes the target's apparent signature. Obscurants can also reduce the radiated signal being emitted toward a target. Obscurants are either smokes or chaff, depending on the type of sensor (spectral band) to be obscured. The relative effects of obscurants such as a conventional battlefield smoke (fog oil) and chaff on sensors is illustrated in *Figure 4-7*.



4.3.1 Visual and IR Obscurants

Smokes, such as white phosphorus, fog oil, HC, and some advanced materials, reduce the atmospheric transmission by scattering or absorbing the light. These processes limit visibility, thus decreasing the signal that reaches the sensor. The reduction in atmospheric transmission is wavelength dependent with longer wavelengths affected less severely than shorter wavelengths. The tuning of smoke is accomplished by controlling the particle size. Since smoke is tuned, a smoke that severely impacts a visible or SWIR system may have little effect on the LWIR systems. Smokes are limited by their persistencies and variabilities. After a period of time, the smoke dissipates, thereby lowering its effectiveness. Also, smoke is not uniform in consistency. There can be variations in smoke concentration, seen as "holes" in the smoke, through which a sensor can operate.

The development of threat doctrine may require a more detailed description of the use of smokes on the battlefield than the scenarios used by the materiel developer and the operational tester. For instance, smoke can be used as a reactive CM emitted once incoming weapons have been detected. Reducing the smart weapon's detectability could prevent the dispense of the smoke. In contrast to this reactive use of smoke is the use of preplanned smoke screens, particularly in the attack or in mine breaching or river crossing operations. In this case, the smoke cannot be avoided. Although these employment issues may not be addressed in the system specification, they can have a significant impact on system effectiveness.

In specifying the smoke obscurants for modeling, the mass extinction coefficient (α in m^2/g), the concentration (g/m^3), and the path length (m) of the smoke must be provided to determine the atmospheric transmission, which determines the extent to which the "target contrast" is reduced at the sensor. Total atmospheric transmission can be divided into two components: through clear air and through the smoke obscurant. For passive sensors, atmospheric transmission can be expressed as follows:

$$\tau_a = (\tau_{clear air} (\lambda, R)) (e^{-\alpha CL}).$$

The first component represents transmission through clear air and the second represents the transmission due to the obscurant. Transmission through the smoke obscurant depends on the concentration length of the obscurant cloud (CL) and the ability of the particles to scatter and absorb radiation (mass extinction, α). Figure 4-8, which applies to passive sensors, shows an explanation of the smoke cloud concentration length or CL. CL is the product of the smoke concentration in grams per cubic meter and the path length *hrough the cloud in meters. A key point is that a cloud with twice the concentration and half the path length has the same CL, therefore the same obscuring effect as a cloud with half the concentration and twice the path length. Radiation attenuation ability of the smoke particles is given by the mass extinction coefficient, α , which is wavelength dependent. Usually α is largest for visible wavelengths and decreases with increasing wavelength. The larger the α , the more effective the smoke obscurant is at attenuating radiation. Table 4-1 shows the mass extinction coefficient of common smoke obscurants. The aCL of an obscurant is not the only consideration when discussing the obscurant's effectiveness, but it is a useful one. Additionally, the environmental conditions under which the system is to operate must be known. A much simpler way of describing the required smoke is to specify the amount of reduction in transmission to be achieved by the smoke. This takes into account both the smoke characteristics and the environmental conditions of interest. Operationally, smoke can act as a decoy for active or semi-active systems. For these systems, simply specifying the transmission reduction is insufficient. The operational impact on these systems must be addressed in order to develop specifications for the smoke, e.g., "aCL" requirements.

In addition to inducing a transmission loss, smoke can also add path radiance. Path radiance refers to the phenomenon of increasing the background signal by the contribution of the atmosphere between the sensor and the background that is along the path of the sensor LOS, hence the name "path radiance." For clear air and short paths (<5.0 km), the path radiance is small. For smokes and obscurants the path radiance can be high. The path radiance from smokes and obscurants can be either emitted radiance from the obscurant cloud itself, or scattered radiance where some other source emits the radiation and the smoke particles scatter radiation into the sensor.

4.3.2 MMW Obscurants

Chaff is used to deceive radar by either confusing a radar or screening the target from the radar. It is a cloud of reflective or absorptive material that is lofted into the air. Once in the air, the chaff remains suspended for some time and interferes with the radar signals by reradiating or by absorbing the received

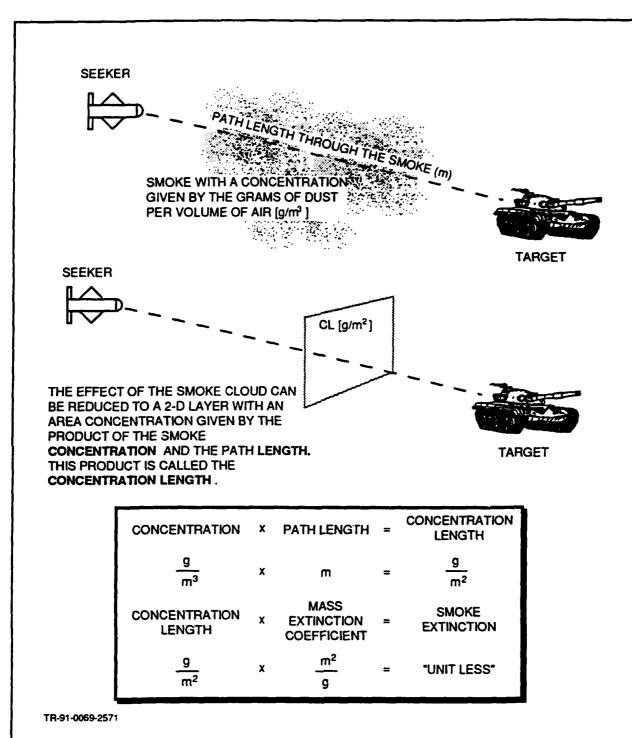


Figure 4-8. Concentration Length of an Obscurant

signals. For RF radars, the chaff is reflective and typically consists of thin metallic wires or foil strips that are resonant at the radar's frequency. Chaff designed to interfere with MMW radar systems may be reflective or absorptive. For MMW radars, reflective chaff is usually metallic-coated glass or fiberglass fibers.

Table 4-1. Mass Extinction Coefficients for Combat-Induced Obscurants²

	Spectral Region				
Obscurant	Visible	SWIR 1.06 µm	MWIR 3 to 5 μm	LWIR 8 to 12 µm	MMW/ Radar ¹
Phosphorous ²	4.08	1.37	0.29	0.38	0.001
HC ²	3.66	2.28	0.19	0.03	0.001
Oil Based	6.85	3.48	0.25	0.02	0.001
Anthracene	6.20	2.50	0.23	0.05	0.001
Vehicular, Artillery (HE) Dust	0.32	0.26	0.27	0.25	0.01 to 0.001
Carbon ³	1.50	1.42	0.75	0.32	0.001
IR Screener	1 to 2	1 to 2	1 to 2	1 to 2	0.01

^{1.} Nominal values; these obscurants are essentially transparent at MMW and radar wavelengths

Reflective chaff works by reradiating or reflecting radiation. A piece of chaff, also called a dipole, is a straight piece of conductive material that acts like a dipole. Theoretically, the optimal length for a dipole reflector is one-half the wavelength of the radiation to be reflected. However, since the chaff material is not a perfect conductor, the actual length would be slightly less than one-half the radar wavelength. The bandwidth response of a dipole can be controlled by adjusting the width, or in the case of a coated fiber, its diameter. By packaging chaff of several different lengths together, a wide range of radar bands can be covered with a single deployment, the tradeoff being wide spectral coverage versus radar cross section.

For a simplistic two dimensional, sparsely filled chaff cloud the total RCS can be approximated by N $(0.15)\lambda^2$, where N is the number of dipoles per unit projected area. The radar return for a single tuned dipole is approximately $(0.15)\lambda^2$, where λ is the wavelength of the radar. However, due to shielding and

^{2.} For 50% relative humidity at 10 °C

^{3.} Carbon from combustion

²Joint Technical Coordinating Group for Munition Effectiveness, <u>Smoke/Obscurants Handbook for the Electro-Optical</u>, <u>Millimeter Wave</u>, and <u>Centimeter Wave Systems Developer</u>, <u>AMSAA</u>, 1 September 1989.

other effects, the RCS of the entire three dimensional chaff cloud is not $(0.15)\lambda^2$ multiplied by the number of dipoles. The RCS of the cloud (σ) has been shown, using classical absorption theory³, to be:

$$\sigma = A_c \left[1 - e^{-N\sigma_0} \right]$$

where A_c is the area of the cloud projected to the radar, N is the number of dipoles per unit projected area of the cloud, and σ_0 is $(0.15)\lambda^2$.

Absorptive chaff absorbs radar signals, therefore attenuating the energy that reaches a target and the energy that is reflected by the target in the direction of the radar (two-way attenuation loss). In absorptive chaff, the fiber length is an order of magnitude smaller than the wavelength to be absorbed. The diameter of such a fiber should be less than the MMW "skin depth" of the fiber material. Ideally, the length-to-diameter ratio should be between 500 and 1000. Chaff of this nature usually has a very low density causing deployment difficulties. "Birdnesting," the condition where clumps of chaff stick together, can be a common problem with absorptive chaff, especially if a more magnetic fiber is used instead of carbon fiber. Grenade launchers are used to deploy the chaff, with cloud effectiveness lasting 10 to 20 seconds, depending on wind conditions.

Reflective chaff is used as a decoy for self-protection measures. A bloom of chaff is launched upon detection of an incoming MMW TGSM in hopes that the target lock will be transferred to the chaff. However, since the velocity of the chaff drops rapidly to zero after deployment, Doppler radar techniques can distinguish between the cloud and a moving vehicle. Also, in order to deploy the chaff optimally, a method for detecting the incoming MMW TGSM is necessary.

For obscurant techniques, either reflective or absorptive chaff is used. In a reflective chaff cloud, radar detection is denied if the power returned per resolution cell is greater than the power returned from the target. Absorptive chaff attenuates the radar signal preventing the radar from distinguishing the target from the background. For radar absorption, the idea is not to reduce the RCS of the vehicle to zero since this would create a radar "hole," which is as obvious as an unobscured vehicle. Exception is made in the case where the chaff cloud is very large with respect to the target, such that the target is lost in the black hole generated by the chaff cloud. Instead, the goal is to lower the RCS to equal that of the background. Again, the chaff is a reactive CM, and a method for detecting the incoming MMW TGSM is necessary for this type of chaff deployment. For modeling purposes, chaff must be specified by type (reflective or absorptive), material used and size, length of time it remains aloft, and size of the cloud. Typical absorptive chaff characteristics are given in *Table 4-2*^A. Here, L/D is the ratio of length to diameter of the fibers.

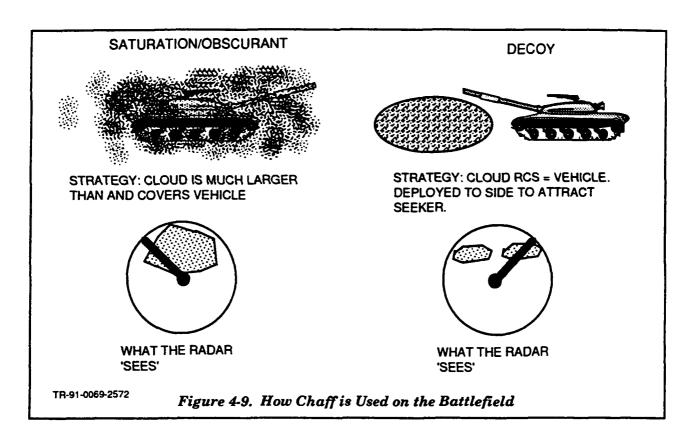
³"The International Countermeasures Handbook," EW Communications, Inc., 1976-77.

⁴"Passive Electronic Countermeasures: Electromagnetic Radiation Absorption Capabilities - Warsaw Pact," DIA, 19 May 1989.

Table 4-2. Radar Attenuation for Carbon Fiber Chaff

L/D	D (mm)	Number of Dipoles in Reference Cube	Loss (dB)	Bandwidth (GHz)
1000	0.1	125,000	-11	2-150
1000	0.2	62,500	-11	2-75
1000	0.3	41,667	-11	2-50
1000	0.4	31,250	-11	2-38

Reference cube: 6.25-kg of fibers within \bar{a} 50 m cube (1.25 x 10⁵ m³)

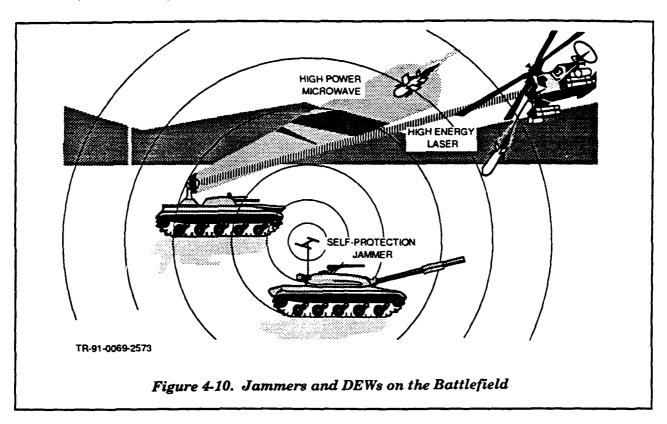


4.4 JAMMERS AND DEWS

Jammers and DEWs are devices that transmit beams of radiation, which can be pointed at targets, for the purpose of interfering with, disturbing, exploiting, deceiving, masking, or otherwise degrading the reception of other signals that are used by smart weapon systems⁵. They are controlled in frequency, energy, waveform, and duration. For these CMs to be effective, knowledge of an incoming smart weapons's

⁵"Vulnerability of Smart Munitions to Directed Energy Weapons," AMSMI-RD-SM, 14 April 1988.

operation, such as frequency, is desired; however, this obviously does not apply to hard kills. Since a signal is transmitted by jammers and DEWs, these CMs should be used in a reactive manner. Otherwise, the jammers/DEWs emissions would lead to their own detection by other weapon systems. The survivable solution would be a stand-off jammer (SOJ) which would radiate for specific periods of time. Two major DEWs are projected for tactical applications at this time: HPMs and HELs. Also, discussed in Subsection 4.4.2 is the notion of using gun/fired projectiles and missiles as DEWs. Both DEW systems and jammers may be pulsed or continuous wave (CW) and cause different effects depending on frequency, energy, waveform, and duration. The goal of a DEW is to deposit enough energy into the target to induce smart weapon failure. Figure 4-10 depicts a scenario with jammers and DEWs.



4.4.1 Jammers

4.4.1.1 Visual and IR Jammers

Several techniques exist for visual and IR jamming. For visual systems, flares can be used as jammers. TV seekers normally have an automatic light control or gain control that adjusts the gain based on the orightest object in the FOV. Therefore, if a target pops a flare into the FOV of the TV seeker, the gain is adjusted around the flare emission. Consequently, everything except the flare is blackened, which causes difficulty in detection. Noncoherent IR jammers can be effective against SWIR systems. Weapon systems that use SWIR beacons for missile tracking can be jammed by a strobe operating at the correct frequency. The strobe emits a signal that is seen by the SWIR beacon tracker. The automatic tracker

adjusts the missile's aimpoint based on this signal. Depending on the placement of the strobe, large miss distances can result.

4.4.1.2 MMW Jammers

MMW TGSM systems have a significant advantage in reducing the effects of CMs due to their inherent characteristics. These characteristics include narrow, directive beam patterns with low sidelobe patterns, high atmospheric attenuation at certain MMW frequencies, and short-range applications. All of these conditions provide the MMW TGSM with transmission security for covert operation, which would reduce the range at which the TGSM is detected and the jammer reaction time. The high atmospheric losses and the antenna characteristics will limit the use of SOJs and probably require a jammer with a moderate to small beamwidth, which brings forth requirements for pointing and tracking the jammer system. Currently, proven electronic counter-countermeasure (ECCM) techniques such as pulse compression, spread spectrum, and frequency agility can make MMW systems even more resistant to CMs. Provided that the jammer is able to overcome these issues, the techniques used for MMW CMs tend to be extensions of those that have been thoroughly evaluated at microwave frequencies. These jamming techniques can be divided into three categories: power jamming, noise jamming, and function jamming.

Power jamming is the use of high-power transmitters to saturate the seeker's receiver, thus hiding the target return under a larger energy transmission. Some of these jammers use high-energy pulses to maintain a fluctuation in the seeker automatic gain control (AGC) which reduces the seeker's ability to track the target. Examples of the electronic countermeasure (ECM) techniques used for this type of jamming are SOJs and self-screening blinking jammers.

Noise jamming uses multiple, low-power transmitters to provide a background in which the real target cannot be detected from false targets or clutter. Examples of this type of jamming are barrage noise jamming, broadband noise jamming, swept, smart, repeater jammers, continuous wave jammers, pulse jammers, spot noise jamming, cooperative blinking jamming, and expendable decoy jamming.

Function jamming uses ECM equipment to receive, analyze, duplicate, and retransmit the seeker signals in any available manner that disrupts the search and tracking operations. Examples of this type are multiple target presentation jamming, velocity gate pull-off (VGPO) jamming, range gate pull-off (RGPO) jamming, amplitude modulation jamming, and cross-pole or cross-eye jamming. Several excellent basic references on jamming are available.^{6,7}

⁶Van Brunt, Leroy B., "Applied ECM," Volume I, EW Engineering, Inc., 1978.

⁷Button, Kenneth J. and James C. Wiltse, ed., <u>IR and MMW: Vol. IV MMW Systems</u>, Academic Press, 1981.

4.4.2 **DEWs and Projectiles**

DEWs are devices that transmit directed beams of EM radiation at incoming smart weapons. Projectiles are devices that fire a missile or bullet at the incoming smart weapon. DEWs and projectiles are being discussed together because of three common characteristics. Both are threatening the physical survivability of the smart weapon, not just the functional survivability, both require an extensive fire control subsystem for effective operation, and both are unlikely, for many reasons, to be seen on the battlefield and are therefore assigned to the Category III CM.

For effective operation of DEW and projectile CMs, an extensive fire control sensor suite and battle management computer is required. The term extensive is used relative to a simple radar warning receiver that is required for a chaff grenade to launch. The fire control sensor suite will have to search wide areas, detect the incoming SMs or GMs, track individual munitions, determine the targeting priorities, prepare a battle engagement plan that utilizes itself and other DEW or projectile systems, setup firing solutions, engage the smart weapons, perform damage or kill assessment, and continue to update the battle engagement plan. DEWs and in particular HELs by their nature require a very specialized fire control function called beam control. The beam control function points, focuses, and maintains the beam on target through out the engagement. This paragraph is intend to demonstrate the difficulty in developing DEW and projectile CMs. However, before dismissing this type all together, it must be emphasized that the fire control issues are difficult but not impossible. The Navy's Phallanx gun system is a fielded example of a projectile-based CM. The key point is that DEWs and projectile-based CMs are in the Category Ill, potential category of threat CMs.

4.4.2.1 HPMs

Microwave and MMW radiation occurs in the EM spectrum between the frequencies of 300 MHz and 300 GHz, with the 1 to 100-GHz range used for weapons applications due to atmospheric propagation considerations, power requirements, antenna size, and energy coupling requirements at the target. HPMs can be affective against both MMW and IR sensors. The mirrors in an IR seeker reflect and focus microwave energy just as well as the IR energy. The degree of effectiveness will be related to the coupling of the microwave energy into the sensor electronics. More on coupling will be discussed in this section. HPM as a CM may accomplish its mission by achieving either a soft kill or a hard kill. A hard kill causes mission failure through structural damage. A soft kill causes the smart weapon to fail in its mission by temporarily or permanently disrupting the electronic systems or sensor. Some examples of possible HPM hard and soft kills are listed below.

HARD KILL

Surface-induced plasma shock

Plasma heating

Thermal heating

Radome blow-off (missile and aircraft radomes)

Electronics burnout

SOFT KILL

Electronics upset

EO sensor degradation

G&C disruption

Biological disruption (guided munition operator)

Limited experiments of HPM hard-kill mechanisms can be conducted in the home. By placing aluminum foil, metal objects, and even one's calculator in the average microwave oven, one can see examples of HPM hard-kill mechanisms. (Note: AMC-SWMO is not responsible for any damage done to the microwave oven or objects placed in the oven.) Fundamentally, HPM hard-kill damage will result from the excitation of electrons in conductive components in the weapon. The incident radiation will setup high current densities in the electron plasmas. High current densities will cause ohmic (resistive) heating of the conductors. High current densities could also cause sparking at points where the surface electrical fields are strongest (sharp edges and pin points). The excessive heating within the missile by conductive components will eventually cause the component to fail, or cause a neighboring nonconductive component to heat and then fail. Microwave ovens have no effect on most ceramic plates. However, a common experience has been to burn oneself handling a plate of food that has been heated in the microwave. The microwaves did not heat the plate. The microwaves heat the food, the heat from the food makes the plate hot. (For technical accuracy, the mechanism for heating food in a microwave is due to the excitation of the rotational states of water molecules in the food, not the electron plasma.) Hard-kill damage from HPMs can therefore include: structural damage, melting of components, shorting out electronics, fusing and immobilizing moving parts, and damaging the antenna or optics to the point of making the sensor inoperable.

The primary mechanism for soft kill with HPM will be electronics upset. Electronic upset is defined as the temporary impairment of system operation, which occurs when the energy coupled into the system either masks normal electrical signals or generates false signals that interfere with the normal operating

signals of the system. Electronic burnout is permanent damage resulting from thermal overload due to the absorption of microwave energy and arcing or dielectric breakdown caused by a high-voltage surge.

The energy required to achieve soft kill may be coupled into the system by either of two paths, referred to as the front-door and back-door paths. The front-door path allows the energy to enter through the energy collector used for normal operation of the sensor. In RF systems, this is the antenna; in systems using IR guidance, this can be the optics. The optical dome may pass, and even magnify, HPM energy into the system. For the IR system, this would be front-door, out-of-band, coupling. The back-door path uses the apertures in equipment housings, seams in TGSM skins, and power supply leads to couple the energy into the system. The best coupling occurs when the wavelength of the HPM is approximately equal to or smaller than the size of the entry point.

HPMs will impact all subfunctions of the smart weapons deliver/engagement function. Depending on the point at which the HPM radiation is received and the type of electronics upset that occurs, the submunitions may not dispense properly due to damage to the altimeter or G&C unit, target acquisition may fail, target lock-on may be broken, or the fuze may fail to activate or may activate prematurely.

To model the effects of HPM on smart weapons, the frequency, power, and type (pulsed or CW) must be known. Additionally, the path must be specified. If a back-door path is used, the tolerances on the seams, the placement of the apertures, and the location of the internal electronics on the smart weapon must also be known. HDL has developed an HPM model, Directed Microwave Energy Weapon Simulation (DMEWS), and maintains a piece-part susceptibility data base on HPMs (see Appendix C).

The issue of soft kill on weapon systems by electromagnetic radiation is covered in a specific topic called special electromagnetic interference (SEMI). In designing a system, attention must be given to SEMI so that the basic design avoids features that enhance the coupling of unwanted EM energy into the system. Mature systems will undergo extensive electromagnetic interference (EMI) testing to ensure weapon system survivability. Numerous references on SEMI and EMI avoidance design guidelines are available. 9.10

⁸*DoD Methodology Guidelines for High Power Microwave Susceptibility Assessments,* OSD-HPM, DDV-90-0017, January 1990.

⁹"Electromagnetic Capability," Engineering Design Handbook, March 1977.

¹⁰"Hardening Weapon Systems Against RF Energy," Engineering Design Handbook, February 1972.

4.4.2.2 HELS

HELs are considered a threat primarily to IR and EO/laser seekers and sensors since the in-band laser intensity (i.e., radiation within the spectral band of the sensor) may be magnified greatly by the optical system of the seeker. This means that the detector elements may burnout or intermediate optical elements may be crazed or melted at sufficiently high power levels. At lower power levels, the detector element may be overloaded causing the sensor to become "dazed." Dazing is just a temporary failure in the sensor. It can be caused by saturating detectors or by "tricking" signal processing such as AGC. In addition to these damage mechanisms, the laser may cause structural damage to the smar' weapon through the heating of the external casing if the range is sufficiently short and the laser power sufficiently high. Out-of-band damage to the seeker dome may occur at sufficiently high laser power levels. For example, a MWIR seeker dome may be crazed or melted by a high-power SWIR laser. Likewise, the same hard kill could be achieved against a MMW TGSM.

There are several lasers that can be used as DEWs. Examples of such lasers and their operating regions follow. The Nd:YAG (neodymium: yttruim aluminum garnet) laser operates in the SWIR band at $1.06~\mu m$ or frequency doubled (to one-half the wavelength at $0.53~\mu m$). The CO₂ (carbon dioxide) laser is a high-power laser operating at $10.6~\mu m$ in the LWIR region. Chemical lasers, such as hydrogen fluoride (HF) and deuterium fluoride (DF), operate in the MWIR. However, fielding chemical lasers on the battlefield is not yet practical. Other potential laser weapons are the laser range finder and laser designator. These lasers could be used as jammers/DEWs by directing them at incoming munitions or GM launchers.

There is a limitation to the power output of HELs due to the process of thermal blooming. Over long distances, the effect of thermal blooming is a larger beam pattern with a lower intensity at the mainbeam. Because of this decrease in energy, a longer dwell time is required to achieve damage to the system. Lasers will affect both the acquire and hit functions of smart weapons. The laser may temporarily or permanently blind the seeker to prevent acquisition and hit.

Modeling the effects of lasers on smart weapon components or systems requires knowledge of the laser's wavelength and power at the target. This implies that the laser energy, duration (pulse length or dwell time) of interaction with the target, and the environment through which the laser is propagating are specified.

4.4.2.3 Projectile-Based CMs

This subsection is being added for completeness. The key points to be made are that projectile-based CMs will destroy incoming smart weapons by virtue of kinetic impact with the round, debris from the round and warhead, or from the warhead energy. Approaches may include using a massive amount of dumb bullets to form a wall of steel, or using a smart bullet to track and hit the incoming smart weapon. A

third approach could utilize a floating or hovering object between the SM and target vehicle that appears as a target and prevents the SM from hitting its intended target. It seems quite natural that, as smart weapon technologies advance both with friendly and threat forces, the best weapon against a smart weapon will be another smart weapon. Some further classified comments on threat projectile-based CMs and the fire control sensors that are required are supplied in Volume II of this series, "Effects of Countermeasures on Smart Weapon Technologies," January 1992.

5. ENHANCING SMART WEAPON EFFECTIVENESS IN A CM ENVIRONMENT

In this section, basic concepts and issues are examined that address how smart weapons can overcome the various CMs that are present in the battlefield. A CM is a device, technique, or action that responds to a specific enemy action or capability; a CM is designed to reduce an enemy's capability or operational effectiveness. CCMs are devices, techniques, or actions designed to permit a system to function effectively even in the presence of threat CMs. This section is a discussion of smart weapon CCMs. CCMs for smart weapon systems are unique to the system and the CM being countered. While the specifics of these techniques are not covered in this overview report, a discussion of the general types of CCMs and their implications to smart weapons development is useful. This section addresses basic CCM techniques that can be developed for smart weapons, the hardware and software design, and employment and engagement options. The discussion of CCM techniques will be divided between CCMs that address CM effects and CCMs that address the CM function. The purpose of the section is to present the subject of smart weapon CCMs in a broad perspective such that the combat developer, materiel developer, and decision maker can gain a better understanding of how smart weapons can overcome CMs.

5.1 SMART WEAPON CCM TECHNIQUES

Specific hardware components and software algorithms designed to overcome CMs are varied and numerous. However, all can be characterized as either countering the CM's effect on the weapon system or countering the functional operation of the CM. Within each broad characterization, the CCM techniques can be either offensive or defensive. A MMW-TGSM with a HOJ capability designed to destroy a RF jammer or HPM weapon is an example of an offensive CCM that counters the functional operation of the CM. A hardened dome could be designed for a Bat submunition that could withstand direct radiation from a HEL. Since the HEL is attempting to crack or craze the dome of the seeker, this would be an example of a defensive CCM that counters the effect of the CM. Both of these broad characterizations will be discussed, along with the implications to smart weapons development.

5.1.1 Countering CM Effects

All CMs are designed to produce an effect on the performance of the smart weapon. Obviously, the overall effect is the degradation of the weapon performance or virtual elimination of the weapon system. Most of the more effective CCMs are those that treat the effects of the CM and not the CM itself. *Table 5-1* lists some examples of CMs, their effects, and the potential CCMs that address the effect. It must be realized that these are merely potential CCMs - they may not actually be developed. For example, the CCM that uses adaptable signal processing to select an optimal aimpoint against a variety of target appearances will actually be very complex and time-consuming to develop, if it can be done at all. Several of the CCMs listed are case limited, such as increasing transmitter power for an active sensor to counter target signature

alteration. This could be an effective CCM if it is signal-to-noise limited, but will be ineffective if it is signal-to-interference limited.

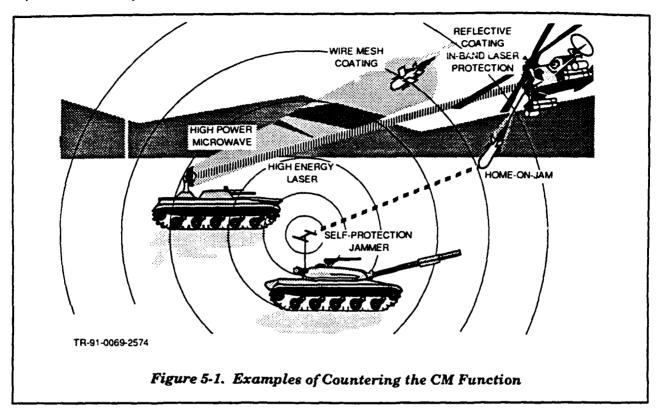
Table 5-1. Examples of Potential Ways of Countering CM Effects

СМ	Possible Effect on the Smart Weapon Sensor	Potential CCM to CM Effect
Target Signature Suppression	Lower/less detectable target signature; reduced probability of detection, classification, and kill	Reduce sensor noise Increase detector sensitivity Increase transmitter power for an active sensor Improve signal processing to filter out more clutter, making sensor more sensitive Larger aperture/antenna to improve sensor sensitivity/gain
Target Signature Modification or Augmentation	Primary impact would be to alter aimpoint selection and tracking, due to a distorted signature. Distorted target signature could also affect detection/classification if altered target features were being used as a detection/classification discriminant.	Adaptable signal processing that can select an optimal aimpoint against a variety of target appearances Develop larger set of image templates
HEL/HPM	Crazing and cracking of domes, destruction of electronic components, and electronics upset	Overall sensor hardening Harder dome materials Specialized radiation hardened electronics components Improved design (electronics and structure)
Decoys	Sensor detects and engages decoy, thus wasting weapon on a nontarget. Further effects include: aimpoint distortion, increased false alarm rate, and break track.	Use multiple discriminates to detect and classify target, thus forcing greater fidelity in a decoy to look more like the target and therefore, more costly Temperature (two-color IR) Size (finer resolution) Temporal (frame-to-frame correlation) Polarization (polarimetric MMW seeker)

5.1.2 Countering CM Functions

The intent of CCMs that counter the CM function is to either destroy the CM that causes the effect or to negate the CM by disrupting a critical function. *Figure 5-1* illustrates how a CCM would counter a CM function. The most direct approach would be to attack and negate the CM itself. As mentioned earlier a home-on-jam (HOJ) capability would negate the jammer or HPM weapon. Trying to directly eliminate

foliage on tanks by shooting it off is unreasonable, but eliminating heated corner cubes, towed decoys, and replicas with a volley of conventional munitions could be effective.



Smart weapons are employed as families of systems (e.g., Dragon, TOW, Hellfire, and Copperhead), yet oftentimes the vulnerabilities of smart weapons and the resulting specification will view the smart weapon of interest as the only smart weapon on the battlefield. For example, in the case implied above, a mix of dumb and smart weapons can be a very effective smart weapon CCM. The dumb munitions would have the effect of stripping off and disabling many of the more complex CMs (decoys, corner cubes, etc.). Also, since the dumb munitions would have a greater lethality against unarmored vehicles, the net result following such an attack would be to increase the ratio of armored to unarmored combat vehicles in the array for the SMs. The extent and reliance of such a weapons mix for a CCM will be established by the combat developer (i.e., TRADOC). Thus, it is important that the proponent combat developer consider the full family of smart weapons and the mix of weapons on the battlefield.

As implied by the name of this class of CCM, negating the CM does not necessarily imply directly attacking it. Much like a smart weapon, a CM requires various components to function, and if one of the components can be made to fail, the CM can be negated. One example would be to defeat the function of an in-band laser weapon by placing a filter on the surface of the outer optics. In-band lasers are designed to take advantage of the optical gain provided by the sensor telescope to concentrate a lethal or blinding

level of radiation on a susceptible component (i.e., a detector). The filter, which would be selected to operate at the frequency of the in-band laser, would prevent the radiation from entering into the system. Thus, one of the CM functions - optical amplification by the sensor - has been negated.

Another example applies to reactive CMs. Generally a reactive CM requires the detection of the smart weapon before the CM is activated. An example of a reactive CM would be a chaff dispenser on a tank designed to detect incident MMW radiation then dispense the chaff. In the case of a HEL or HPM threat, the system must acquire and track the incoming TGSM in order to hit it. If the TGSM can reduce its signature or reduce its exposed timeline to the extent that the HEL/HPM cannot find the TGSM in time to negate it, then the CCM has operated effectively.

5.2 SMART WEAPON HARDWARE/SOFTWARE DESIGN

In developing and assessing options to improve both the survivability and availability of the smart weapon, the materiel developer must address as many CCMs as possible. Many times, solutions to CM vulnerabilities require little in hardware or software redesign. Sometimes the solutions may require minor additions to the system, such as a wire mesh coating on an optical dome to keep out RF radiation. Other times, the solution may only require a change in operation. For example, when a FLIR is temporarily not in use, the scan mirror might be stopped and locked into a position where it projects the unfocused scene onto the side of the optical cavity. This would make it invulnerable to in-band laser radiation during periods when the operator is not looking through the eyepiece. Finally, it must be recognized that some CMs can only be negated by making a specific and potentially costly design change to the system. Most modern IR seekers are no longer vulnerable to simple flare decoys. Achieving that level of survivability has universally required the addition of a second spectral band. Although this technique is becoming more common and more mature, the bottom line is that a two-color seeker is more complex and costly than a single-color seeker. Had IR decoys not been a viable threat, the simplicity of the single-color detector would be extremely popular.

Whether the materiel developer (or contractor) is designing a smart weapon system or developing a smart weapon concept, all potential CCM design options should be examined in a tradeoff analysis. It is assumed that it has been determined that organizational or operational changes are inadequate to overcome the vulnerability and a system design change or new system is in order. To ensure that all potential design options are considered, the specific CM must be fully understood. The first and most important step is to identify the category that the CM will be assigned to and the level of performance that will be required in the presence of the CM. The second step is to fully characterize the functionality of the CM. The third step is to fully characterize the effect of the CM on the system.

In coordination with several other agencies, SMO recommends the performance level required for each identified CM. The intelligence community, i.e., DCSINT, Army Intelligence Agency (AIA), etc., will have the ultimate authority to assign the CM to a category. This means that the PM has limited control and influence over the assignment of a specific CM to a category. Category III CMs only require the PM to consider growth options (P3I programs) and he is not required to divert substantial resources to them. Category I CMs will require the smart weapon system to perform at the required levels for this category.

Section 4 of this volume provides technical information on various CMs and their effects. This should be used as a guide and not a substitute for fully discussing the specific CM with knowledgeable experts. Oftentimes, simple CCMs are overlooked because both the function of the CM and the effect of the CM on the sensor were not fully understood and a key CM function or effect that could be easily overcome was missed. By fully examining how the CM functions and its effects on the sensor, the PM/contractor can devise the most effective CCM.

The advanced signal processing characteristic of smart weapons tends to be the most common area of system design changes for removing system vulnerabilities. As target signatures are altered and decoys are employed, it appears possible to defeat the CM by modifying the affected algorithm. Although software changes will continue to be the CCM of choice, they should be scrutinized on several points. First, software is not free. Much of the expense of developing new algorithms (software) for a smart weapon comes from retesting its performance. Second, increasing software complexity requires additional processing capability. DoD policy is to maintain a 50% processing load utilization to allow for future expansion of the signal processing. The reserve processing is intended to accommodate software increases as the system moves through development. In addition to the increase in processing hardware, the CCM algorithm may require additional time on the smart weapon engagement timeline to function. The point is that algorithm enhancements to defeat CCMs will cost something. This is not to imply that they are too costly, only that the developer must fully examine the impact to the system for the CCM being considered.

The versatility of software and algorithms used in smart weapons has also generated the concept of reprogrammability. Weapon system reprogrammability is now a Army mandated requirement. As stated by the Vice Chief of Staff of the Army, "It is DA policy that all smart/brilliant munitions and sensors which require target recognition to function possess a reprogramming capability unless specifically waived by HQDA".¹¹ "Reprogrammability is the ability to reconfigure system operation through modifications to

¹¹Subject: "Smart Munitions Reprogramming Policy and Signatures Collection/ Dissemination Concepts for Smart Munitions/Sensors," VCSA Policy Letter (DACS-ZB), 30 January 1989.

system software". ¹² Reprogrammability gives the smart weapon system the flexibility to respond with software CCMs to newly encountered CMs or changes in targets and/or tactics.

Although the versatility of reprogrammability is a viable CCM approach, it is not a solution but a means to a solution. Because SMs must be reprogrammable, the issue of CCM effectiveness goes beyond the performance of the specific CCM algorithm or operational software. Some considerations must be given to how this example of reprogrammability will be supported. A process must be established to determine which set of programs is to be down loaded into the SM. This process includes the collection of timely and critical intelligence data and decision logic (i.e., tactical decision aids), which selects the software to be used. Although the battlefield intelligence gathering and dissemination resources may be extensive, they are limited and oftentimes so conditionalized that they lose value. Therefore, the application of reprogrammability must include the availability of the intelligence resources during the time the weapon system is fielded. To take advantage of reprogrammability, intelligence resources must provide battle damage assement (BDA) feedback regarding target status after engagement and/or information as to whether or not a smart weapon hit the intended target(s).

5.3 SMART WEAPON EMPLOYMENT AND ENGAGEMENT OPTIONS

The entry of GMs and SMs into the Army inventory is by no means characterized by the development of a single weapon system. GMs and SMs are represented by families of systems. Examples include: direct fire (Javelin, TOW, LOSAT, STAFF, Longbow, and Hellfire) and indirect fire (Bat, SADARM, MLRS-TGW, and Copperhead). Furthermore, smart weapon carriers and launch platforms, combined with reprogrammability, provide the system with enhanced employment and engagement options that gain system CM robustness beyond the performance of the seeker alone. It is imperative that the smart weapon PM check that the requirements community and the evaluation community consider these enhancements when preparing evaluations and assessments. Again, each susceptibility must be considered on a case by case basis. Employment and engagement options are not broad sweeping CCMs that negate all projected CMs and reported vulnerabilities. Each of these options will be discussed in more detail.

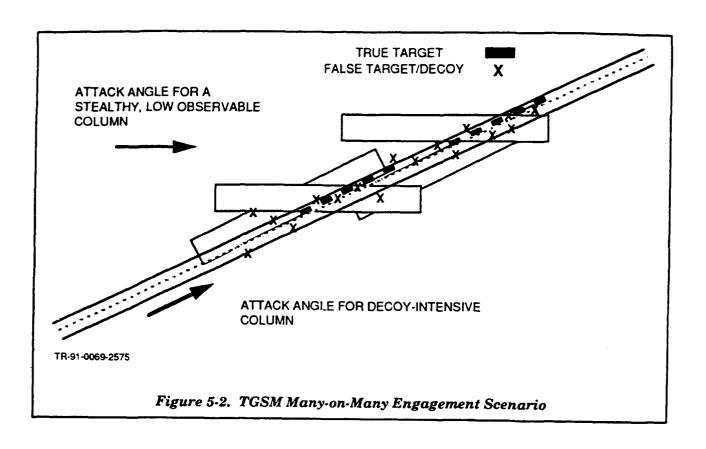
A common engagement issue is the extent and type of threat CM resources. Again, caution must be used to prevent under-specifying a system. However, it is also the PM's responsibility (along with the CM community) to check that the system is not over-specified. A single weapon system should not be expected to engage a threat that has all its CM resources devoted to defeating the weapon system. The number of smoke/chaff cannisters that a T-72 can carry is limited; however, the obscurant combinations can be carried that are effective from visible to MMW. If only MMW smart weapons were employed on the

¹²"Smart Weapons Reprogrammability Assessments and Recommendations," AMC-SWMO, 1 July 1990.

includes systems that operate from the visible to the MMW, thus forcing the threat to allocate CM resources accordingly.

With respect to type of CMs, the multispectral family of smart weapons makes the job of the threat much more difficult. A CM that is effective in one spectral region may, in fact, cause enhanced smart weapon performance in another band. The materiel and combat developers, along with the experts in the threat, assessment, and analysis communities must understand the effect of a CM against the family of smart weapons. If a CM is projected for use by the threat, then its degrading and enhancing effects must be taken together. Currently, there does not exist a single dirty battlefield template that provides a standard list of CMs. Further, there is no formalized process in the requirements community to crosswalk survivability annexes for consistency of CM specifications. Survivability annexes, STARs, and vulnerability assessments are done on a system-by-system basis and not on a collection of systems. SWMO has previously reviewed and crosswalked survivability annexes, and is a good resource for providing this kind of support if requested by a PM or combat developer.

One of the first steps taken to defeat a battlefield vulnerability is to consider operational changes in the employment of the SM. Naturally, one of the ways in which smart weapons can maintain CM robustness is to provide for a high degree of operational flexibility. This can be obtained through reprogrammability and by exploiting the launcher/carrier flight profile flexibility. Figure 5-2 shows some of the advantages in array angle of attack options that a TGSM can use. As a case in point, consider the use of decoys - both towed and reactive. Although a threat tank column would attempt to remain covert and, if engaged, survivable, there are some obvious tradeoffs between the use or nonuse of decoys. If the column uses decoys, either fixed along the route or towed, the column gives up covertness, with a subsequent decrease in target location error (TLE) by friendly target array detection assets. In return, the array is gaining survivability because the decoys will draw off TGSMs from the real targets. This threat option might be countered by a smart munition by taking advantage of the decreased TLE and engaging the array along the axis of the column. This would allow the TGSM multiple target opportunities and time over the array to perform sophisticated, time-consuming discrimination algorithms to defeat the effect of the decoy. In contrast, a stealthy target array that made maximum use of signature alteration and no use of decoys would have a larger TLE due to the difficulty in maintaining contact with the array by the surveillance assets. In this case, a smart munition engagement along the axis of the array could be disastrous, since a large TLE could cause the munition's footprint to run parallel to the array and not cover any targets. An engagement that was more perpendicular to the axis would be more robust for this case.



6. SMART WEAPON CM PROGRAM PLANNING ISSUES

In this section, some of the issues associated with how CM survivability is incorporated into smart weapon development programs will be discussed. Both mature programs in systems development as well as technology base programs are included. Most of the issues presented in this section will be under the direct purview of the project office. The issues related to threat CMs must be addressed early and continuously in the weapon system acquisition process. The success of the entire program may depend on how well CMs have been considered in the design and development of the smart weapon system. The PM is charged with the sole responsibility for developing the smart weapon system; therefore, the PM must ensure the adequacy of specifications and meaningfulness of test results.

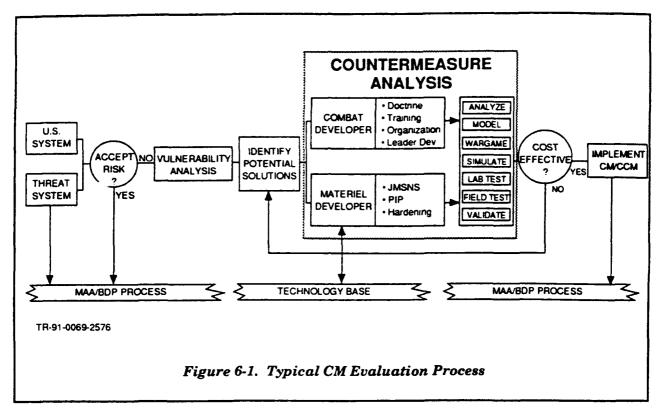
The PM is not alone in this process; SMO, VLAMO, VAL and others in the CM community are charged with supporting the PM. However, the PM must not be a passive participant, accepting annexes (requirements) or test results without the intention of ever challenging them. Early and continual coordination must be maintained with all members of the CM community to insure that requirements are meaningful and test plans will address the evolving system design. Further, the PM has the fiscal resources to fund CM support efforts.

This document addresses several issues of system survivability as they apply to smart weapons. However, the basic issue is not whether the smart weapon lives to fight another day, but rather if it survives long enough to perform its function for the majority of the time. In this context, it is more an issue of system availability in a CM environment than an issue of system survivability.

It is prudent at this point to digress and emphasize the necessity to maintain program security through the use of a program operational security plan. Maintaining strict security control on aspects of the system that could lead to a vulnerability is vital. Failure to do so could result in fielding of a responsive threat CM to the system before the system itself is fielded.

6.1 REQUIREMENTS AND SYSTEM SPECIFICATION DEFINITION

Both combat and materiel developers have a role in the development and specification of system capabilities that relate to threat CMs. The process that each PM goes through to fix a CM problem is not always the same. Very often, the CM process is tailored to fit unique program goals or is designed to accommodate special requirements (priorities, limited time, immediate need). A typical CM process is depicted in *Figure 6-1*.

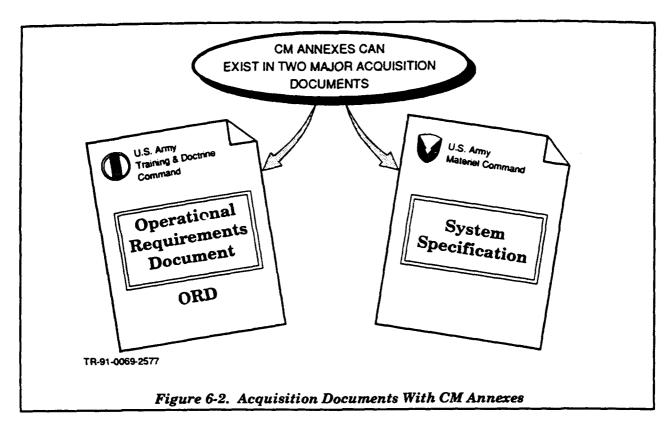


The CM process in the figure portrays the major steps that a PM must consider before implementing a CM fix in a system. Two important decision points are included in the process that relate to the level of acceptable risk to the system and the cost-effectiveness of the potential solution. If the risk to the system is unacceptable, the degree of vulnerability must be determined and potential fixes identified. If the cost to fix the system is prohibitive, then the PM must reevaluate the range of potential solutions.

Solutions to threat CMs are not always hardware-oriented solutions. The combat developer must consider the impact of altering doctrine or tactics, individual and unit training, organizational restructuring, and leader development. Each of these has a significant impact on the battlefield employment of a US smart weapon system and each may contribute to the reduction of a system's vulnerability (or its ultimate survivability). The CM analysis includes a wide variety of tools to explore and validate potential system modifications and enhancements.

A major program document that supports the materiel development process is the STAR. The STAR is prepared by the supporting FID. It contains detailed information on factors related to threat CMs, as well as data on threat system capabilities.

The CM requirements are normally contained in both the ORD and the system specification document (*Figure 6-2*). An annex to these documents is the preferred, but not required, method of addressing the threat CMs.



The ORD focuses on the operational employment issues and user expectations as they apply to the smart weapons CM capability. The ORD is not intended to provide detailed system characteristics and specifications. Based on the operational requirements outlined in the ORD by the combat developer, the materiel developer translates these needs into the more detailed System Specification.

People in the CCM (hardening) business are often frustrated by the difficulty of having CCM features incorporated into initial weapon system designs. Normally, a weapon is frozen in design to meet its specified threat. However, it takes a long time to develop and field a weapon system, and the threat frequently changes over that time as the potential enemy upgrades or incorporates new CMs into his systems. As these changes occur, appropriate CCMs may be to incorporated into system designs or product improvements may be made to fielded systems.

To address this situation, the impact of CMs on US system design and development has been related to the threat CM categories. The three categories of CMs are defined in Subsection 3.1.2. The CM categories were established by the SMO to provide guidance to PMs regarding their responsibility to address threat CMs in the development of their systems.

Categories I, II, and III outline the basic requirements to be considered as part of the materiel acquisition process for incorporating hardware/software fixes in a new system to negate or reduce threat CM effects.

- 1. Category I CMs must be negated in the first production run of a weapon system. The system must perform at the levels stated for Category I CMs.
- Category II CMs may allow a slight reduction in system-level performance in the presence of that CM. There is also the possibility that tradeoffs may be managed between cost and risk to protect the system against Category II CMs. Otherwise, first production runs must meet the stated system-level performance for this CM category.
- 3. Category III CMs allow susceptibilities to exist during the first production of the system; however, a P³I program must be developed at the conceptual level to enhance system performance in the presence of this CM. Some Category III CMs may not be DSCINT approved. Further, some performance against some Category III CMs might be required in initial production runs.

6.2 SYSTEM DESIGN SUPPORT

The smart weapon CM/CCM design process is one of designing a system to maintain the required level of performance against the stated CMs. As discussed in Section 5, enhancing or maintaining smart weapon performance in a CM environment can be accomplished by countering the CM effects or countering the CM function. Before the design process can consider CCM alternatives, the CM effects and the CM function must be fully understood. Section 4 and Appendix C of this volume can be used as an initial starting point for this analysis. Whether the PM is considering or evaluating a proposed system design, or the prime contractor is developing a design solution to a CM, both the function of the CM and the effect of the CM must be fully presented. Oftentimes the current modeling of this phenomenon is too simplistic or the understanding of the CM by key decision makers is too cursory. As smart weapon sensors and signal processing become more complex, so will the CMs and the characterization of the CMs.

During the PM-sponsored CM Working Groups, it would be beneficial to spend time discussing and reviewing the CM effects on the system and its function, as they relate to the current set of engineering models and design tools that are being used. Likewise, in the formulation of technology base programs, it is imperative that the CM effects and functionality modeling be reviewed for adequacy as they relate to the emerging program. In addition to reviewing the system design and supporting analysis tools, if inadequacies in the specification are discovered, they need to be discussed at the next specification review. This is not stating that as new system susceptibilities are realized they should be automatically added to the survivability annex. If a system design or tradeoff is being based on a CM characteristic that was not addressed in the survivability annex, it should be added at the next milestone review. The PM should then establish a working requirement and document it as such. For example, a TGSM system aimpoint selection and tracking routine might be based on a key signature attribute such as a pattern of hot spots or scatterers. The survivability annex might state that Category I signature alteration techniques will reduce the overall signature, but make no statement as to the specific aimpoint selection signature attribute. This is a case where the specific signature alteration technique must be investigated to see if it alters the attribute, the

system must be assessed as to the impact of a varied pattern or signature attribute. Any effects must be incorporated into the engineering model, and the resulting CM issues must be incorporated by the next iteration of the specification. Again, the point must be emphasized that the working assumption is that the CM was in the survivability annex as a DCSINT-approved CM, but that a full characterization of the CM as it affected the system is lacking.

6.3 **TESTING ISSUES**

Detailed and quantifiable data in the CM descriptions and characterizations must also support smart weapon testing. Technical descriptions of CMs are necessary for developing the Test Evaluation Master Plan (TEMP). It must be realized that when developmental and operational testing take place, with respect to CM testing, the stated requirements will not be a guideline, but an edict. Unless the original specification addressed the testing of the CM, the test entrance and exit criteria will be difficult to define and the conditions of the performance results will be questionable. The PM must take a proactive role during the preparation of the CM specification data to ensure that testing of the CMs is considered. Some of the issues are:

Instrumentation

- How are the CM levels measured (interfering or noninterfering) and what is the testing accuracy?

Measurement procedures - They must be consistent to ensure repeatability and consistency. Thus, any variability recorded in a CM level is a function of the CM and instrument noise, not the operator who was performing the procedure.

Test criteria

- What are the ranges and minimum acceptable performance levels of CMs for test entrance criteria? For example, how much smoke is required for testing in smoke, and what is considered too much smoke, or what smoke is required to meet the weapon system performance threshold. Can pass/fail exit criteria be established?

System performance

- What are the performance estimating procedures for determining system performance at various levels of CMs?

The trend in DoD wiil be to continue to combine developmental and operational testing. The specification must provide the specifics and details necessary to allow for the analytical evaluation process. but also allow flexibility during the process of testing. The basis for the flexibility is not to create a test that is easy for the system or even one that is not too hard. The flexibility acknowledges the real world issues that occur in the field. Target signatures change, obscurants have varying thicknesses, foliage catches on fire, it rains, and the wind changes direction. What is required is a clear understanding of how the performance of the system will be assessed based on the test results with varying degrees of conditions for the purpose of determining the exit criteria.

6.4 CM AND WEATHER AVAILABILITY ANALYSIS

The statement of required system availability in CMs and weather and the evaluation of this availability will be the primary responsibility of the combat developer and AMSAA, respectively. However, the PM must ensure that the required statement of availability in both CM and weather conditions is clear and unambiguous. As comically depicted in *Figure 6-3*, the statement of required availability can be easily confused when combined with required levels of effectiveness and weather. As part of the rationale for the survivability annex, the technique that will be used to calculate availability should be documented. It also needs to be recognized that in building a system to a specification, all affected parties are assuming the risk that the stated requirements reflect the expected performance in the field. The associated risks will be the fielding of a system that fails to meet expectations or the cancelling of a system that would have met field performance expectations.

The stated conditions under which the system is expected to perform must include the combined occurrence and mixes of weather, CMs, and pattlefield-induced effects. Collectively, these describe the dirty battlefield. The AMC-SWMO "Weather Specification Guide" discussed the issues associated with creating and defining weather states for determining system availability. The process for defining the weather states is complex but rather straightforward with regard to procedure. The process for defining CM environments is much more involved and will be coordinated by the proponent combat developer with inputs from SMO, among others. Of specific concern to the PM is the statement of expected performance and method by which it will be determined. In the case of GMs, such as Javelin, the key effectiveness figure of merit might be effective range; for SMs, such as Bat, the key effectiveness figure of merit might be the number of combat vehicles killed out of a specific target array (e.g., tank battalion). In either case, the statement of availability should address the following to be meaningful to the system developer:

- 1. Quantifiable statement of the minimum acceptable, key effectiveness figures of merit.
- 2. A clear definition of the non-CM environment to include dirty battlefield effects.
- 3. A clear definition of the Routine (Category I) CM environment and how Category I CMs are mixed and/or combined; and how they are mixed with the non-CM environment.
- 4. A clear definition of the Less Frequent (Category II) CM environment and how Category II CMs are mixed and/or combined with each other, Category I CMs, and the non-CM environment.
- 5. A clear statement of how the CM environments are expected to be combined with weather states (i.e., should smoke be expected with heavy fog conditions or with high wind speed conditions).

DECISION MAKING...WEATHER AND SUBMUNITION PERFORMANCE



WE'VE SPECIFIED WEATHER AND SUBMUNITION REQUIREMENTS, MR. SECRETARY



SUBMUNITIONS WILL BE A' AIL ABLE 80% OF THE TIME IN ALL SEASONS



OF COURSE, SUBMUNITIONS WILL NOT BE AVAILABLE 20% OF THE TIME



BUT WE WILL ALLOW 25% DEGRADATION 10% OF THE TIME



WE ALSO DESIRE NO MORE THAN 50% DEGRADATION 20% OF THE TIME...



DO YOU SUPPORT OUR DECISION?

95% OF ME IS 50% CONFUSED. 5% OF ME IS 100% CONFUSED.

TR-91-0069-2556

Figure 6-3. The Difficulty in Stating Clear Availability Requirements

Particularly in the case of submunitions in a many-on-many example, the nonlinear effects of the engagement will produce different results depending on how stated countermeasure mixes and combinations are interpreted. For simplification of the following example, consider a TGSM that can detect all clean targets but cannot detect targets that use countermeasures. Clean targets occur with a 80% probability and camouflaged targets occur with a 20% probability. If the environments are assumed to be combined, then 80% of the time all targets will be clean and 20% of the time all of the targets will be camouflaged. In this case, the TGSM will be effective only 80% of the time. However, if the environments are mixed, 80% of the targets will be clean and 20% of the targets will be camouflaged at any given time. For this case, none of the camouflaged targets will be detected but there will still be an ample number of detectable targets for the munitions. Therefore, the system will be effective 100% of the time. This illustrated the importance of clearly stating a specific mixing and/or combining of environments in the survivability annex.

In calculating the availability of smart weapons in CMs and weather environments, a proposed approach is to use the matrix format shown in *Table 6-1*. This matrix is offered as a reasonable example, but is also applicable for defining the mixes of weather and CMs. The weather states listed along the side are those that are appropriate for the system, the ones shown are based on an Infrared Terminally Guided Submunition (IRTGSM). The "Weather Specification Guide" discusses this process in much more detail. The first CM environment is the "Routine Category I CM," as there is no "non-CM" environment. This CM environment also includes battlefield-induced effects. The "Less Frequent Category II CM" environment is the "Routine Category I CM" environment plus the mix of Category II CMs. This must include the percentage of targets having the CM or the probability of encountering them. Finally, the "Potential Category III CM" environment, along with the densities on the battlefield or the probability of occurrence. For the "Potential Category III CM" environment, only a qualitative assessment will be done as these are not DCSINT-approved CMs.

The weather environments must have the probability of occurrence listed. This is a number derived from the regional/seasonal/diurnal climatic data base (see the "Weather Specification Guide"). The CM environments need either a priority, probability of occurrence, or other weighting factor, which must correlate to the statement or required availability given in the ORD. Thus, by quantitatively calculating the key performance figure of merit for each cell in the matrix, an estimate of system availability can be made and compared to the requirement.

¹³ Smart Weapons Weather Specification Guide," AMC-SWMO, 31 October 1990.

Table 6-1. Strawman CM and Weather Availability Matrix

CM Env Wx State	Category I Routine and Dirty Battlefield	Category I + II Less Frequent	Category I + II + III Potential			
Clear	For each cell in matrix the following must be addressed either quantitatively or qualitatively					
Clouds	Wx state description CM environment description Combined Wx/CM effect CMs degraded by weather CCMs degraded by weather Remove CMs that are incompatible (e.g., a Category I CM)					
Clouds with Precipitation						
Clear with Ground Fog						
Clouds with Fog						
Wx: Weather eff Env: Environmen	* =					

7. SUMMARY

This "Guide to How Countermeasures Affect Smart Weapons" and the companion classified "Effects of CMs on Smart Weapons Technology" are the first in a four volume series of CM-related studies and reports sponsored by the AMC-SWMO. AMC-SWMO has Army management oversight responsibilities for smart weapon technologies and issues. This responsibility includes ensuring an adequate understanding and appreciation of the importance of CM planning in smart weapon research, development, and testing. The technological chess match between smart weapons and the CMs to those smart weapons is now beginning in earnest. A coordinated team effort requires community education and an opening of communication channels.

This guide has provided some clarifications and insights of the responsibilities and roles of the various Army agencies involved in CM and/or smart weapon planning (Sections 1, 2, and 6). As roles, missions, and organizations change, the community must communicate those changes, especially with regard to the entry points between the combat and material developers and the intelligence specialists. The sequences of activities must also be better clarified. If there are suggestions for improving the coverage of these important programmatic processes in this text, convey them to the AMC-SWMO.

Another issue defined during the preparation of this guide and the companion classified volume was the need for consistency and clarity in the statement of CM categories and types in the various program documents. Details must be provided to support the design, testing, and evaluation process. Section 4 of this volume discussed the technical details and issues that are required to characterize CMs. Section 6 addressed the necessity of updating the ORD, system specification, and TEMP as a result the evolving system design. The ORD may use different terminology from the TEMP or the system specification, but the terminology must be traceable and, where appropriate, quantified. In test documents, a range of levels (e.g., smoke densities) is appropriate to address uncertainties in the threat specifics and the realities of variability in test conditions. As program documents are produced or modified, the CM descriptions must be traced into all other program documentation to ensure the smart weapon is developed and tested adequately.

One of the purposes of the AMC-SWMO CM program is to increase the flow and availability of CM test data. Many CM models and data bases exist with varying controls and coverage. Section 4 and Appendix C of this volume discussed the technical data that is available to quantify and model the effects of CMs. Volume II of this series provides further classified data. Currently, there does not exist an integrated CM effects database or library of models.

Survivability annexes are periodically reviewed for threat traceability. They should also be reviewed for testability (See Subsection 6.3). Do they provide smart weapon CM specifications or guidance

to guarantee integrity and thoroughness in the testing? Are test results repeatable and comparable? Survivability annexes for smart weapons must also be reviewed for adequacy and clarity for simulation and modeling and, of course, for design efforts. This review is essential to preclude "smoke" being light/transient in the design and heavy/persistent in the testing or vice-versa.

Categories of CMs (Routine, Less Frequent, and Potential) were introduced by SMO to clarify CM design requirements for the PMs. As currently defined, all smart weapon performance thresholds must be met in the initial production system in the presence of Routine (Category I) CMs. For Category II (Less Frequent), similar demands are placed on performance thresholds, but criteria can be adjusted or waived with justification. If these definitions are different from those used in previously published smart weapons program documents (TEMPs, Contract Specifications, etc.), they should be reviewed and corrected.

Category III (Potential) CMs are useful as a design consideration in smart weapon designs, but the lack of DCSINT approval is a Catch 22. They could be used by program detractors to discredit the program objectives or products. Specific guidance is needed for the level of resources or the extent of P³I planning required of the smart weapon PM.

Developing survivable, effective, CM-robust smart weapons is a challenging task within DoD's RDT&E process. System vulnerability reporting to the Army System Acquisition Review Council/Defense Acquisition Board (ASARC/DAB) decision makers demands the experience and credibility of a dedicated organization. In the Army, VLAMO currently performs this function. AMC-SWMO's oversight role for smart weapons overlaps with VLAMO's (and SMO's, etc.) roles; their coordination on areas of mutual interest is essential. Overlaping and duplicating efforts in important and complex subjects are common and are healthy. Developing survivable smart weapons demands everyone's involvement. When a system fails, the entire Army loses.

REFERENCES

- 1. "Burle Electro-Optics Handbook," Burle Technologies, FOH-11, 1974.
- 2. Joint Technical Coordinating Group for Munition Effectiveness, <u>Smoke/Obscurants Handbook for the Electro-Optical</u>, <u>Millimeter Wave</u>, and <u>Centimeter Wave</u> Systems <u>Developer</u>, <u>AMSAA</u>, 1 September 1989.
- 3. "The International Countermeasures Handbook," EW Communications, Inc., 1976-77.
- 4. "Passive Electronic Countermeasures: Electromagnetic Radiation Absorption Capabilities Warsaw Pact," DIA, 19 May 1989.
- 5. "Vulnerability of Smart Munitions to Directed Energy Weapons," AMSMI-RD-SM, 14 April 1988.
- 6. Van Brunt, Leroy B., "Applied ECM," Volume I, EW Engineering, Inc., 1978.
- 7. Button, Kenneth J. and James C. Wiltse, ed., <u>IR and MMW; Vol. IV MMW Systems</u>, Academic Press, 1981.
- 8. "DoD Methouology Guidelines for High Power Microwave Susceptibility Assessments," OSD-HPM, DDV-90-0017, January 1990.
- 9. "Electromagnetic Capability," Engineering Design Handbook, March 1977.
- 10. "Hardening Weapon Systems Against RF Energy," Engineering Design Handbook, February 1972.
- 11. Subject: "Smart Munitions Reprogramming Policy and Signatures Collection/ Dissemination Concepts for Smart Munitions/Sensors," VCSA Policy Letter (DACS-ZB), 30 January 1989.
- 12. "Smart Weapons Reprogrammability Assessments and Recommendations," AMC-SWMO, 1 July 1990.
- 13. "Smart Weapons Weather Specification Guide," AMC-SWMO, 31 October 1990.

APPENDIX A. INDEX TO KEY POINTS

APPENDIX A. INDEX TO KEY POINTS

I. Understanding the current set of players in the CM community and their roles

SMO - Coordinates Requirements

VLAMO - Coordinates Assessments

VAL - Performs EW Vulnerability Assessment

BRL - Performs Ballistic Vulnerability Assessments

See Section 2.3

II. Understanding the current Vulnerability Assessment process, and definitions and implications of CM categories (Categories I, II, III)

Category I CM - Routine

Category II CM - Less Frequent

Category III CM - Potential

See Sections 7.1 and 7.2

III. Make assurances for the proper and complete technical specification of CMs

Signature Alteration - Section 5.1

Decoy/Deception - Section 5.2

Obscurants - Section 5.3

Jammers and DEWs - Section 5.4

Testing - Section 7.3

See Sections 5, 7.2, and 7.3

IV. Use of the current CM related models and databases

Signature Alteration - TABILS/TRISIG (C.11)

Obscurants - AAODL (C.4), EOSAEL (C.3)

Jammers and DEWs - DMEWS (C.6)

V. Planning for CM/CCM in the smart weapon system development

At the time of conducting this study, the DoD was reformulating the DoD 5000 series directives governing the system acquisition process. Furthermore, AMC was planning a major reorganization involving LABCOM and many of the commodity commands (AVSCOM, MICOM, AMCCOM, etc.). Discussion of specific organizations to plan for CM testing and assessment is premature, given this pending

reorganization and reassignment of responsibilities. However, certain CM/CCM planning fundamentals should remain pertinent in the future. The key fundamental is necessity of the PM to form a CM-TIWG. Membership on the CM-TIWG should include, as a minimum representatives from:

PM and Prime Contractor

Proponent RDEC

Proponent TSM/Combat Developer

VAL

SMO

AMSAA

Areas covered by the CM-TIWG and appropriately reviewed are:

How CMs are specified

- adequacy of technical description
- completeness/consistency
- clear statement of required performance
- ORD and system specification annexes

How CMs are modeled

- physical models (if appropriate)
- engineering models
- effectiveness models

How CMs are tested

- TEMPS
- entrance and exit criteria
- how they are measured
- model validation

How system CCMs are addressing CMs

- will desired CCM effect by realizable?
- is the assessed risk appropriate?

See Section 7

APPENDIX B. ACRONYMS AND DEFINITIONS

APPENDIX B. ACRONYMS AND DEFINITIONS

α Mass extinction coefficient describes the radiation scattering ability of smoke particles.

AAODL Atmospheric Aerosol and Optics Data Library

AAWS-M Advanced Antitank Weapon System - Medium (became Javelin)

AGC automatic gain control

Active CM A CM that emits a signal or signature. A non-passive CM.

AIA Army Intelligence Agency

AMC-SWMO Army Materiel Command Smart Weapons Management Office

AMCCOM Armaments, Munitions, and Chemical Command

AMSAA Army Materiel Command Systems Analysis Activity

APGM Autonomous Precision Guided Munition

ASARC Army System Acquisition Review Council

ASL Atmospheric Sciences Laboratory

ASM Armored Systems Modernization

BDA Battle Damage Assessment

BDP Battlefield Development Plan

BICT Battlefield Induced Contaminants Test

BRL Ballistics Research Laboratory

C³I command, control, communications, and intelligence

CAC Combined Arms Command (previously Center)

CCM counter-countermeasure

CG Commanding General

Chicken Little Joint Air Force/Army munition test and evaluation program, office at Eglin Air Force

Base

CL Concentration length is the product of the smoke concentration (g/m³) and the path

length through the smoke (m).

CLFO JPO Chicken Little Follow-on Joint Project Office

CM countermeasure

CNVEO Center for Night Vision and Electro-Optics, also CCNVEO, CECOM

COEA cost and operational effectiveness analysis

C Celsius, a unit of temperature

CO₂ carbon dioxide

COMBIC Combined Battlefield Induced Obscurations Code

CRDEC Chemical Research, Development, and Engineering Center

CW continuous wave

dazed A temporary condition in which the sensor can not acquire or maintain track.

DA Department of the Army

DAB Defense Acquisition Board

dB Decibels-A dimensionless measure of the ratio of two power levels, equal to 10 times

the logarithm to the base 10 of the ratio of the two powers P1/P2.

DCG Deputy Commanding General

DCG(RDA) Deputy Commanding General for Research, Development, and Acquisition

DCSINT Deputy Chief of Staff for Intelligence

DEW directed energy weapon

DF deuterium fluoride

DMEWS Directed Microwave Energy Weapon Simulation

DoD Department of Defense

DPICM dual-purpose improved conventional munitions

ε When speaking in terms of the MMW region, it is permittivity (dielectric constant), which

characterizes the effect of the atomic and molecular dipoles of a material.

ε When speaking in terms of the IR region, it is the emissivity, which is defined as the

ratio of the radiance of a given body to that of a blackbody.

ECCM electronic counter-countermeasure

ECM electronic countermeasure

EFP explosively formed penetrator

EM electromagnetic

EMD engineering and manufacturing development

EME electromagnetic effects

EMI electromagnetic interference

EO electro-optic

EOSAEL Electro-Optic Systems Atmospheric Effects Library

ETDL Electronics Technology and Devices Laboratory

EW electronic warfare

EWVA Electronic Warfare Vulnerability Assessment

FAR false alarm rate, yield the number of false targets that will be detected by a sensor in a

given interval of time

FID Foreign Intelligence Division

FIO Foreign Intelligence Office

FITTE fire-induced transmission and turbulence effects

FLIR forward-looking infrared

FOV field of view

frequency A characteristic of electromagnetic radiation and sound. It is the number of harmonic

cycles that 13peat every second.

g gram

GACIAC Guidance and Control Information Analysis Center

G&C guidance and control

GHz gigahertz

GM guided munition

HC Hexachloroethane (type of smoke)

HDL Harry Diamond Laboratories

HE high explosive

HEL high-energy laser

HF hydrogen fluoride

HOJ home-on-jam

IOC

HPM high power microwave

IFOV instantaneous field of view Intensity watts per steradian (W/sr)

IR infrared: 1 to 14 microns

IRTGSM Infrared Terminally Guided Submunition

JMSNS Justification for Major System New Start

JSGCC Joint Services Guidance and Control Committee

initial operational capability

JTCG-ME Joint Technical Coordinating Group for Munitions Effectiveness

K Kelvin, a unit of temperature.

kg kilograms

L radiance (W/cm²-sr)

LABCOM Laboratory Command

LEL low-energy laser

LOS line-of-sight

LOSAT line of sight antitank

LWIR long-wave infrared, generally from 7.5 to 15.0 microns

meters m

Permeability measures the effect of the atoms comprising the material. μ

micrometers um

Mission Area Analysis MAA

megahertz MHz

MICOM Missile Command

MLRS-TGW Multiple Launch Rocket System - Terminal Guidance Warhead

millimeters mm

millimeter wave **MMW**

Materials Technology Laboratory MTL

MWIR mid-wave IR, generally from 3.0 to 5.0 microns

NADR National Armor/Anti-armor Data Respository

Nd:YAG A laser composed of neodymium (Nd) doped into a host crystal of yttrium aluminum

garnet (YAG).

NG/FS next generation/future system

NLOS non-line-of-sight

OPTEC Operational Test and Evaluation Command

ORD Operational Requirements Document

OSD Office of Secretary of Defense

Pacq probability of acquisition

 P^3 I pre-planned product improvement

Passive CM A CM that does not emit a signal or signature; a nonactive CM.

Process Action Team PAT

PEO **Program Executive Office PGM** precision guided munition

Product Improvement Program PIP

PM Program Manager

point of contact POC

The reflectivity of the surface. R&D

research and development

RAM radar absorbing material

RCS Radar cross section: defined at 4 times the ratio of the power per unit solid angle

scattered back toward the transmitter to the power per unit area striking the target.

RDEC Research, Development, and Engineering Center

RDT&E research, development, test, and evaluation

reactive CM A CM that is initiated in battle in response to a perceived threat or threat action.

responsive threat A threat (CM) developed and fielded due to the actual or planned fielding of a system

susceptible to that threat (CM)

RF radio frequency

RGPO range gate pull-off

ROC required operational capability

σ radar cross section

SADARM Search and Destroy Armor Munition

SEMI Special ElectroMagnetic Interference, addresses the EW susceptibility of weapon

system electronics due to incident EM radiation. Focus is on how the radiation is

coupled from the surface to the electrical components.

SFM sensor fuzed munition

skin depth Depth within a conductor at which an electromagnetic wave is damped to 1/e of its initial

amplitude upon entering the conductor.

SM smart munition

SMO Survivability Management Office

SOJ standoff jammer

STAFF Smart Target Activated Fire and Forget

STAR System Threat Assessment Report

survivability The ability to avoid or withstand the effects of enemy action and continue the effective

performance of the mission. Includes both "physical survivability" and "functional

survivability".

SWIR short wave infrared, generally from 0.8 to 2.0 microns.

TABILS Target and Background Information Library System

TACOM Tank Automotive Command

TEMP Test Evaluation Master Plan

TGSM terminally guided submunition

TIWG Test Integration Working Group

TLE target location error

TOW Tube launched Optically tracked Wire Guided

TRAC TRADOC Analysis Command

TRADOC Training and Doctrine Command

transmittance The percent of radiation that propagates from one point to another.

TRISIG Tri-Service Signatures Data Base

TSM TRADOC System Manager

UAV unmanned aerial vehicle

VAL Vulnerability Assessment Laboratory

VGPO velocity gate pull-off

visible The spectral region that is sensitive to the human eye, 0.4 to 0.7 microns.

VLAMO Vulnerability/Lethality Assessment Management Office

wavelength A characteristic of electromagnetic radiation and sound. It is the length of the harmonic

cycle.

WP white phosphorous

WSMR White Sands Missile Range

APPENDIX C. RESOURCE ORGANIZATIONS

APPENDIX C. RESOURCE ORGANIZATIONS

C.1 INTRODUCTION

This appendix presents some of the organizations whose resources are valuable in the CM community.

C.2 ARMY MATERIEL COMMAND - SMART WEAPONS MANAGEMENT OFFICE (AMC-SWMO)

The AMC-SWMO serves as the AMC focal point for the oversight of smart weapon programs for requirements, tech base activities, and proof-of-principle phases in the acquisition phases. The MICOM has been designated by the commander of AMC as the lead command within AMC on smart weapons. The Commanding General (CG), MICOM is therefore designated as AMC Executive Agent for smart weapons and reports to the Deputy Commanding General (DCG) for Research, Development, and Acquisition (DCGRDA). AMC-SWMO reports to the CG, MICOM on all matters concerning the smart weapons developments both internal and external to AMC. AMC-SWMO's mission is to:

- 1. Provide management oversight in the planning, technical evaluating, recommending, and coordinating of smart weapon programs;
- 2. Execute, in selected cases, smart weapon system development programs or tech base programs for key smart weapon-related components;
- 3. Plan and execute, for the Army, the Chicken Little Follow-on Joint (Army and Air Force) Project Office, where the Director of AMC-SWMO serves as the Army's Co-Chairman of the CLFO JPO steering committee; and
- 4. Act as DA focal point for threat signature requirements.
- Perform technical management of the DoD of the Guidance and Control Information and Analysis Center (GACIAC) under the auspices to the Joint Services Guidance and Control Committee (JSGCC)

In performing its function, AMC-SWMO will coordinate with the major AMC subordinate commands (LABCOM, AMCCOM, Tank Automotive Command (TACOM), etc.), TRADOC combat development directorates, and smart weapon responsible PEOs. Among the major activities within AMC-SWMO are the formulation of the Smart Weapon Tech Base Investment Strategy, the review of AMC next generation/future system (NG/FS) smart weapon concepts prior to submission to TRADOC, and the development of the Smart Weapons Master Plan. AMC-SWMO produces a number of products for the smart weapons development communities. This series is one of several prepared by AMC-SWMO. Similar products have been developed for weather, target signatures, smart weapon component technologies, and smart weapon development planning.

Commander
US Army Materiel Command
Smart Weapons Management Office
ATTN: AMSMI-SW
Redstone Arsenal, AL 35898-5222

C.3 ARMY MATERIEL SYSTEMS ANALYSIS ACTIVITY (AMSAA)

AMSAA serves as the AMC lead activity for system analysis, cost, and operational effectiveness analysis (COEA) input data, and reliability and maintainability methodology. AMSAA mission is: to develop and provide to the Army a basis of information and understanding, primarily concerning system performance, effectiveness, support, and integration in terms of capabilities and limitations. This information is then used to support decisions throughout the acquisition lifecycle, which provides the Army with proper materiel. Additional functions related to smart weapon development are as follows:

- 1. Perform test design and independent evaluation for decisions on materiel systems such as combat vehicles and missiles:
- 2. Provide systems analysis support to AMC major subordinate commands and project/product managers;
- 3. Maintain cognizance of performance of fielded equipment through participation in materiel readiness reviews, sample data and field data collection efforts, and special field surveys;
- 4. Serve as the AMC field activity for administering the Tri-Service Joint Technical Coordinating Group for Munitions Effectiveness (JTCG-ME).

In carrying out its mission, AMSAA communicates directly with HQ DA, HQ AMC, PEOs, project/product managers, and other AMC commands and activities. AMSAA utilizes a variety of modeling techniques, ranging from system engineering level to force-on-force, in order to evaluate system performance. Inquiries should be addressed to:

Director, USAMSAA

ATTN: (AMXSY-G) (for ground systems)
ATTN: (AMXSY-A) (for air systems)
Aberdeen Proving Ground, MD 21005-5071

C.4 ATMOSPHERIC SCIENCES LABORATORY (ASL)

The ASL, part of the US Army LABCOM, employs the Army's weather experts. ASL models are incorporated into a large library made up of essentially autonomous models. This library, the Electro-Optic Systems Atmospheric Effects Library (EOSAEL), was first developed in the late 1970s. The latest version is EOSAEL 87. Version 2.0 of EOSAEL 87, also known as EOSAEL 89, was released in March 1990.

The EOSAEL models can be roughly divided into six categories based on the atmospheric characteristics that are modeled. These categories are atmospheric gases, battlefield aerosols, laser propagation, natural aerosols, refractive transfer, and system performance. The names of the modules associated with each category are shown in *Table C-1*. For a good overall description of these categories and the modules, see <u>EOSAEL 87</u>: Volume 1. Executive Summary.

Table C-1. EOSAEL Modules

Atmospheric	Battlefield	Laser	Natural	Refractive	System
Gases	Aerosols	Propagation	Aerosols	Transfer	Performance
LOWTRAN LZTRAN NMMW	COMBIC SABRE KWIK GRNADE FITTE MPLUME	IMTURB NOVAE	XSCALE CLIMAT CLTRAN COPTER	FCLOUD OVRCST MSCAT ASCAT ILUMA FASCAT GSCAT LASS REFRAC	TARGAC RADAR

The modules dealing with battlefield aerosols model the dust and smoke clouds and the missile plumes found on the battlefield. The fire-induced transmission and turbulence effects (FITTE) module predicts the effects of fires and fire plumes on EM propagation; or when running the FGLOW option, it predicts the radiant image of a fire or fire plume segment that will be seen by an imaging system. The fires represent localized sources of burning diesel fuel, motor oil, and rubber. FITTE predicts the LOS path-integrated particulate concentration, the transmittance between target and observer, and both the attenuated thermal radiance from the target and the path radiance at the observer position. If the calculation is performed for a single wavelength, the model predicts the effects of turbulence on a laser beam of that wavelength. The FGLOW option performs calculations for a set of LOS and creates a file of path radiance values that represent the radiant image that would be seen by an imaging system. An output option allows the image data to be transformed to apparent temperatures.

Commander/Director
US Army Atmospheric Sciences Laboratory
ATTN: SLCAS-AA
White Sands Missile Range, NM 88002

C.5 CHEMICAL RESEARCH, DEVELOPMENT, ENGINEERING CENTER (CRDEC)

The Atmospheric Aerosol and Optics Data Library (AAODL) provides data for the analysis of the use of smokes as a CM against optical sensors. AAODL is maintained by the ASL and the CRDEC. To access AAODL, either ASL or CRDEC should be contacted at one of the following addresses.

Commander
US Army Chemical Research, Development & Engineering Center
ATTN: SMCCR-MUC/Mr. Robert Laughman
Aberdeen Proving Ground, MD 21010-5423
(301) 671-2260

Commander/Director US Army Atmospheric Sciences Laboratory ATTN: SLCAS-AR-M (Dr. Robert Sutherland) White Sands Missile Range, NM 88002-5501 (505) 678-4520/4301; AV 258-3951

Registered users of AAODL receive a quarterly bulletin describing the available data. Tables include the names of tests, dates, locations, obscurant types, types of weather data collected, EO and EM measurement types, data status (whether or not available and the media), sponsoring organization (e.g., ASL), associated documents, and point of contact (POC). AAODL contains collected data that has been used for EO models in EOSAEL. For instance, data collected during the Battlefield Induced Contaminants Test (BICT) were used to construct and validate the Combined Battlefield Induced Obscurations Code (COMBIC) of EOSAEL. *Table C-2* shows an example of a data item description taken from AAODL Bulletin, Voi. 6, No. 1, April 1988.

In this example, the index indicates that the data from SMOKE WEEK VIII, sponsored by PM SMOKE, are available in the form of magnetic tapes as well as printed summaries. In addition, the test is documented in a final report. Obscurations included white phosphorous and fog oil, with dispensing munitions including smoke generators and M76 grenades. A variety of weather and aerosol concentration data were taken. In addition, transmission data were collected.

C.6 CHICKEN LITTLE JOINT PROGRAM OFFICE (CL JPO)

The Joint Munitions Test and Evaluation Program Office, known as Chicken Little, is a joint USAF/ USA program to evaluate advanced SMs against actual threat vehicles. Chicken Little operates and maintains an extensive fleet of threat vehicles to support its core mission and the test and evaluation community. Test activities provide analysis as well as cost and technology leveraging, and they stress realistic environments and CMs. Chicken Little test and analysis activities include warhead lethality, target vulnerability, target signatures, and seeker/sensor performance. Seeker/sensor and signature data collected are placed in the Targets and Background Information Library System (TABILS) data base. Warhead data collected are placed in the National Armor/Anti-armor Data Repository (NADR).

Chicken Little Joint Project Office 3246th Test Wing /EAL Eglin AFB, FL 32542-5000

The TABILS data base is operted by Chicken Little. The TABILS data base contains the largest and most comprehensive collection of IR and MMW target and background signatures data within the DoD. TABILS has been a valuable source of signature data for the DoD sensor community for over a decade.

Table C-2. Example Listing from AAODL Expanded Index

CONTACT	N. MICHAEL FARMER. STC
MENT C	SMOKE WEEK VIII (FINAL REPORT
SPONSOR	SMOKE
STATUS OF OPTI- CAL & ELEC- TROMAG- NETIC DATA	DETAIL, TAPES, PRINTED SUM. MARY, LOADED RINTO
STATUS OF AERO- SOL DATA	DETAIL, TAPES, PRINTED SUM. MARY, LOADED INTO RIM
STATUS OF METEO- ROLOGI- CAL DATA	DETAIL, TAPES, PRINTED SUM: MARY, LOADED INTO RIM
OPTICAL & ELEC. TROMAG. NETIC MEA. SURE.	TRANS (MPTR, DUGWAY, SMART), EMIS. SIONS
AERO. SOL MEA. SURE. MENT	RAS, AP, CHEM IM- PINGER
METEO. ROLOGI. CAL MEA. SUNE. MENT	TOWER, WIND: SPD & DIR, TEMP REL HUM, PRES: SURE, SOL FLUX, PASO,
MUNI: TION LIST	SMKGEN, DUST, M76GRD, CBU88
OBSCU- RANT LIST	FOG OIL, GRAPH. ITE, EAS763, ALU. MINUM, HEWP. DUST, RP
LOCATION	EGLIN AFB, FL
DATES	SMOKE8 MAY 1966
TEST	SMOKE8

The TABILS data bases were originally established in the late 1970s in response to the growing need to systematically identify, archive, and retrieve IR and MMW signature data being collected as part of various ongoing measurement programs. The TABILS data base currently comprises 6 IR-related data bases and 13 MMW-related data bases. In addition to TABILS, TRISIG, a directory of data, models and instrumentation, is available for use by Government and industry developers.

TABILS 3246th Test Wing EAL Eglin AFB, FL 32542-5000

C.7 HARRY DIAMOND LABORATORIES (HDL)

HDL, a part of LABCOM, was designated to chair an HPM effects panel by the HPM executive steering group of the Office of the Secretary of Defense (OSD) in 1986. HDL is responsible for the coordination and direction of HPM effects investigations performed by DoD agencies and other contractors. HDL collects and maintains component response data in the Automated Data Base of Piece-Part Component Response to High Power Microwaves. Additionally, the Directed Microwave Energy Weapon Simulation (DMEWS) was developed and maintained by HDL.

Director
US Army Harry Diamond Laboratories
ATTN: SLCHD-HPM
2800 Powder Mill Road
Adelphi, MD 20783-1197

C.8 SURVIVABILITY MANAGEMENT OFFICE (SMO)

The SMO is the AMC survivability specialist and focal point. It serves as the AMC spokesman for combat survivability policy. SMO provides an organizational capability for integrating related survivability and commands. SMO maintains the integrated AMC Survivability Management Plan. The three principal areas of interest of SMO include ground combat, aviation and air defense, and C3I systems. SMO has the capability to identify survivability enhancement requirements for systems in any of these three general areas of interest. This includes assessing the potential value of new technologies used to enhance combat material survivability. SMO develops specific recommendations for system managers about the technical progress needed for more robust ground combat system performance. The office has the capability to perform combat simulations of force-on-force to validate in-house analyses of system effectiveness.

Director
US Army Survivability Management Office
ATTN: SLCSM-TD
Adelphi, MD 20783-1145

C.9 VULNERABILITY ASSESSMENT LABORATORY (VAL)

The VAL is primarily charged with the EW vulnerability assessment of Army weapon systems. VAL is assigned to the US Army LABCOM, and is thus part of the AMC. VAL is located in WSMR, NM and was formerly known as the Office of Missile Electronic Warfare. Throughout this document, VAL's primary role of EW vulnerability assessment has been the focus. Quite naturally, the laboratory resources and expertise in the EW area apply to other related areas. VAL's missions are:

- 1. Conduct independent EW vulnerability assessments of US Army combat and combat support systems throughout their lifecycle;
- 2. Research, demonstrate, and recommend electronic CCMs (ECCMs) to system developers; and
- 3. Perform EW vulnerability assessments of foreign systems.

In the process of developing CCMs, a valuable source of information for ECCMs is VAL. Further, VAL's primary role of EW assessment, as shown in *Figure 1-1*, should not be construed to be its only role in the CM/survivability community. VAL's mission also makes it a technical contributor and advisor to the intelligence assessments and FIDs. In fact, VAL will be active throughout the CM/survivability community to ensure to the proper integration of ECM threats in to the process. Also, specific information gained by VAL on a weapon system will be under the control of the weapon system PM. To obtain that data, the specific PM must be contacted.

Commander
US Army Vulnerability Assessment Laboratory
ATTN: SLCVA-GC
White Sands Missile Range, NM 88002-5513

C.10 VUNERABILITY/LETHALITY ASSESSMENT MANAGEMENT OFFICE (VLAMO)

The US Army VLAMO is assigned to the US Army LABCOM, and is thus part of the AMC. VLAMO is located at Aberdeen Proving Ground, MD. VLAMO's goal is to ensure timely, well-founded, comprehensive, quantitative, and objective vulnerability and lethality assessments of Army systems. VLAMO's mission includes:

- 1. Act as AMC executive agent for vulnerability and lethality assessments,
- 2. Integrate and coordinate vulnerability assessment planning and resourcing,
- 3. Ensure adequacy and auditability of assessments, and
- 4. Represent synthesized results of vulnerability assessments at major ASARC/DSARC decision milestones.

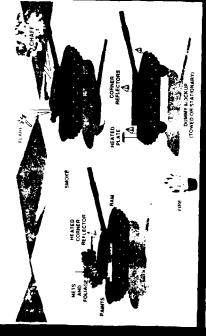
Director
US Army Vulnerability/Lethality Assessment Management Office ATTN: AMSLC-VL-D
Aberdeen Proving Ground, MD 21005-5001

APPENDIX D. EXECUTIVE CHART



COUNTERMEASURE EFFECTS ON SMART WEAPON SENSORS

Signature Meration and Deception



Obscurants



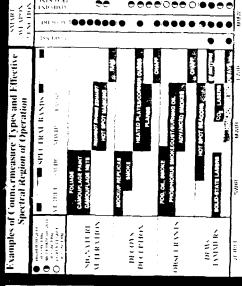
ACCESSIBILITY: SUSCEPTIBILITY VULNERABILITY": FEASIBILITY: PEQUIRES ALL THREE CORDITIONS TO EXIST

WYOURHHABILITY BECLUDES A FOURTH CIRCLE. HITERCEPTABILITY

Ξ

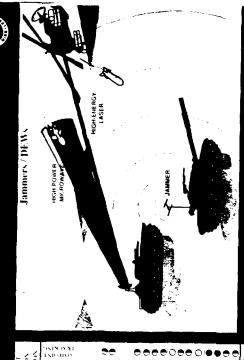
122 Present by Same and Same

FOC AMC-SWMO DRIFF CONTRACT NUMBER DAMINT R9 D 0059



hed production. (Probotominic heads may not be as stringent as would be preferring of CMs are employed in the of CMs may be requested to the feature decidence of the AP ³ Epidepoine decident diapproach Cabegory, LC Max Survivability Annex CM Category Definitions feasible but are not DC'att1 **DCSINT approved CMs that** DCSIM: approved UMs that have a high probability of CMs that are judged to be technically and tartically have a fow to medium probability of being MINIM WILL MILLAN HE QUE NO ROHIM 3.00 MELLIN

APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED



Countermeasures and Survivability Community

EVAL UATIONS OPTEC DCSINT

REQUIREMENTS

N. VLAMO

PEO ASM

INTEGRATION AND COORDINATION

US ARMY MATE 4IEL COMMAND SMART WEAPONS MANAGEMENT OFFICE ATTR: AMSMI SW REDSTONE ARSENAL, AI 35898 COMMANDER (AMC-SWMO)



GUIDANCE AND CONTROL INFORMATION ANALYSIS CENTER (GACIAC)

GACIAC is a DoD Information Analysis Center operated by IIT Research Institute under the technical sponsorship of the Joint Service Guidance and Control Committee with members from OSD, Army, Navy, Air Force, and DARPA. The AMC Smart Weapons Management Office of the U.S. Army Missile Command provides the Contracting Officer's Technical Representative. GACIAC's mission is to assist the weapon guidance and control community by encouraging and facilitating the exchange and dissemination of technical data and information for the purpose of effecting coordination of research, exploratory development, and advanced technology demonstrations. To accomplish this, GACIAC's functions are to:

- Develop a machine-readable bibliographic data base -currently containing over 42,000 entries;
- 2. Collect, review, and store pertinent documents in its field of interest -- the library contains over 15,000 reports;
- 3. Analyze, appraise, and summarize information and data on selected subjects;
- 4. Disseminate information through the GACIAC Bulletin, bibliographies, state-of-art summaries, technology assessments, handbooks, special reports, and conferences;
- 5. Respond to technical inquiries related to weapon guidance and control; and
- 6. Provide technical and administrative support to the Joint Service Guidance and Control Committee (JSGCC).

The products and services of GACIAC are available to qualified industrial users through a subscription plan or individual sales. Government personnel are eligible for products and services under block funding provided by the Army, Navy, Air Force and DARPA. A written request on government stationery is required to receive all the products as a government subscriber.

Further information regarding GACIAC services, products, participation plan, or additional copies of this special report may be obtained by writing or calling: GACIAC, IIT Research Institute, 10 West 35th Street, Chicago, Illinois 60616-3799, Area code 312, 567-4519 or 567-4526; Fax 312, 567-4889.

JOINT SERVICE GUIDANCE AND CONTROL COMMITTEE

